National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

University of Alberta

Embeddings of Rings into Skew Fields

by

Jorge J. Valencia

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Master of Science

in

Mathematics.

Department of Mathematical Sciences

Edmonton, Alberta

Fall 1995

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

THE AUTHOR HAS GRANTED AN IRREVOCABLE NON-EXCLUSIVE LICENCE ALLOWING THE NATIONAL LIBRARY OF CANADA TO REPRODUCE, LOAN, DISTRIBUTE OR SELL COPIES OF HIS/HER THESIS BY ANY MEANS AND IN ANY FORM OR FORMAT, MAKING THIS THESIS AVAILABLE TO INTERESTED PERSONS.

L'AUTEUR A ACCORDE UNE LICENCE IRREVOCABLE ET NON EXCLUSIVE PERMETTANT A LA BIBLIOTHEQUE NATIONALE DU CANADA DE REPRODUIRE, PRETER, DISTRIBUER OU VENDRE DES COPIES DE SA THESE DE QUELQUE MANIERE ET SOUS QUELQUE FORME QUE CE SOIT POUR METTRE DES EXEMPLAIRES DE CETTE THESE A LA DISPOSITION DES PERSONNE INTERESSEES.

THE AUTHOR RETAINS OWNERSHIP OF THE COPYRIGHT IN HIS/HER THESIS. NEITHER THE THESIS NOR SUBSTANTIAL EXTRACTS FROM IT MAY BE PRINTED OR OTHERWISE REPRODUCED WITHOUT HIS/HER PERMISSION.

L'AUTEUR CONSERVE LA PROPRIETE DU DROIT D'AUTEUR QUI PROTEGE SA THESE. NI LA THESE NI DES EXTRAITS SUBSTANTIELS DE CELLE-CI NE DOIVENT ETRE IMPRIMES OU AUTREMENT REPRODUITS SANS SON AUTORISATION.

ISBN 0-612-06550-2

Canada

University of Alberta

Release Form

Name of Author: Jorge J. Valencia

Title of Thesis: Embeddings of Rings into Skew Fields

Degree: Master of Science

Year this Degree Granted: 1995

Permission is hereby granted to the University of Alberta Library to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the thesis, and except as hereinbefore provided neither the thesis nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatever without the author's prior written permission.

(Signed) . . . . . .

Jorge J. Valencia
Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta
T6G 2G1
Canada

Date: . . August 8th

Nadie puede escribir un libro. Para
Que un libro sea verdaderamente,
Se requieren la aurora y el poniente,
Siglos, armas y el mar que une y separa.

Jorge Luis Borges

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Embeddings of Rings into Skew Fields** submitted by Jorge J. Valencia in partial fulfilment of the requirements for the degree of Master of Science in Mathematics.

Dr. H. H. Brungs (Supervisor)

Dr. A. Pianzola (Chair & Examiner)

Dr. H. J. Hoover (External)

Date: July 20/95

To P. A.

Abstract

The goal of this thesis is to describe methods and give examples of embedding a ring in a skew field.

In many parts of Algebra, for instance in Ring Theory, an attempt is made to study and classify the basic building blocks involved with the hope that the more complex structures can then be reconstructed from these fundamental blocks in some manner—for example the Wedderburn–Artin theorem. From this point of view the construction of a new skew field (also called a division ring) is a worthwhile endeavour since the skew fields are the basic building blocks in Ring Theory.

At the end of chapter I, we shall present a family of free algebras of rank two over a given skew field with *countably many non-isomorphic fields of fractions*. The idea of this example is due to Fisher [Fis71], but the proof presented here is original (cf. section I.6 on page 46).

In chapter III, we prove a sort of Cramer's rule for non–commutative

rings due to Cohn [Coh71a]. We also prove lemma III.2.3, on page 127, which is original. It will give us the exact relation between the universal Σ–inverting ring and the Σ–rational closure. As an application of Cramer's rule and this lemma we shall show how to construct epic R–fields from their singular kernels.

The embedding of a *"suitable" ring* in a division ring will provide a way of constructing a skew field; most often, a skew field constructed to embed a ring in it will not be finite dimensional over its center. What is meant by a *"suitable" ring* is the subject matter of this work.

Acknowledgements

With deep pleasure, I wish to express my gratitude to my supervisor, **Dr. Hans H. Brungs**, for his encouragement and advice throughout the preparation of this thesis. Particularly appreciated was his immediate attention to any question I raised to him throughout this year and for the many hours he spent teaching me some of his many "tricks of the trade" every Friday afternoon. I wish on everyone such a pleasant supervisor–student relationship, both mathematically and personally.

I would like to thank the Committee Chair, **Dr. Arturo Pianzola**, for his ***masterful approach*** to the various problems which arose in the preparation of this thesis. I am also grateful to him for the many enjoyable and lively discussions we had during last term, where he pointed out many mistakes, always suggested improvements and made useful comments about the organization of each chapter, for his careful proof–reading of the thesis and for his encouragement. Without him, I would have never finished (or even begun) this Masters Program.

I am indebted to **Leo Creedon** for his excellent proof–reading of this thesis and his suggestions about the preparation of the final version of this work.

Lastly, I want to thank **the Department of Mathematical Sciences and the Mathematics Library at the University of Alberta** for providing the facilities to make this research possible.

Contents

Terminology, notations and conventions

Introduction

I The General Embedding Problem 1

I.1 Fractions 2

I.2 The general embedding problem for monoids 5

I.3 The general embedding problem for rings 19

I.4 Skew polynomial rings 31

I.5 Examples of Skew polynomial rings 41

I.6 Examples of rings with countably many non-isomorphic fields of fractions 46

II The Malcev–Neumann and Cohn embeddings 50

II.1 Ordered groups 52

II.2 The Malcev–Neumann construction 64

II.3 Examples of non-left Ore rings embeddable in fields 75

II.4 Complete topological groups 78

II.5 An embedding theorem for a class of inverse limit semigroups . 87

II.6 Cohn's embedding theorem 91

II.7 Birkhoff–Witt algebras 105

III A general method of embedding 108

III.1 The category of epic R–fields and specializations 113

III.2 The construction of epic R–fields from their singular kernels . . . 122

III.3 The equivalence of epic R–fields and specializations with singular kernels and inclusions 130

III.4 Matrix ideals 133

III.5 Prime matrix ideals and their characterization as singular kernels 140

III.6 General criterion for a ring to be embeddable and to have a universal field of fractions 144

IV Dubrovin's partial solution to a problem of Malcev 149

IV.1 The main idea of Dubrovin's embedding 150

IV.2 Automorphisms of linearly ordered sets 151

IV.3 The universal covering group of $SL(2,\mathbb{R})$ and the module of formal series 152

IV.4 Summable systems and σ–linear, monotone and monomial endomorphisms of the module of formal series 154

IV.5 The complexity 156

IV.6 Fully rational endomorphisms of the module of formal series and conformed decompositions 157

IV.7 Dubrovin's embedding 158

IV.8 Application of Dubrovin's embedding to give a partial solution to Malcev's problem 159

Bibliography 161

Name Index 167

Index 169

Terminology, notations and conventions

For any term used in this thesis without explicit definition, the reader is referred to Hungerford [Hun89], Jacobson [Jac89], Lang [Lan93] or any graduate algebra book at the same level as any of these three books.

All rings occurring are associative, but not necessarily commutative (in fact, the problems considered reduce to trivialities in the commutative case, cf. page 21). Every ring has a unit–element, denoted by 1, which is inherited by subrings, preserved by homomorphisms, and acts as the identity operator on modules.

We note that in a ring $1 = 0$ is possible; it happens precisely when the ring is **trivial**, i.e. a ring with a single element. A ring is said to be **entire** or an **integral domain** if $1 \neq 0$ and the product of non–zero elements is non–zero. In any ring R, the set of non–zero elements is denoted by R^* or by $R^\times$, but this notation is mostly used for integral domains, where R^* is closed under multiplication. If R^* is a group under multiplication, R is called a **field** or **division ring**. Occasionally the prefix "skew" is used, to emphasize that our fields need not be commutative, which means that we must qualify the commutative fields. By an **embedding** of a ring R in a skew field K we mean an injective ring homomorphism $R \longrightarrow K$. An element u in a ring or monoid

is **invertible** or a **unit** if it has an **inverse** u^{-1} satisfying $uu^{-1} = u^{-1}u = 1$. Such an inverse is unique if it exists at all. The units of a ring (or monoid) R form a group, denoted by $\mathcal{U}(R)$. The ring of all $n \times n$ matrices over R is written $\mathcal{M}_n(R)$ or R_n. The set of all square matrices over R is denoted by $\mathcal{M}(R)$. Instead of $\mathcal{U}(R_n)$ we write $GL_n(R)$. An element u of a ring is called a **left zero–divisor** if $u \neq 0$ and $uv = 0$ for some $v \neq 0$; if u is neither 0 nor a left zero–divisor, it is called **right regular**. Corresponding definitions hold with left and right interchanged. A left or right zero–divisor is called a **zero–divisor** and an element that is neither 0 nor a zero–divisor is called **regular**. Over a field a square matrix which is a zero–divisor or 0 is also called **singular**.

Let A be a commutative ring; by an **A–algebra** we understand a ring R which is an A–module such that the multiplication is bilinear. Sometimes we will want a non–commutative coefficient ring A; this means that our ring R is an A–bimodule such that $x(yz) = (xy)z$ for any x, y, z in R or A; this will be called an **A–ring**. To rephrase the definitions, an A–ring is a ring R with a homomorphism $\alpha \mapsto \alpha.1$ of A into R, while an A–algebra is a ring R with a homomorphism of A into the centre of R. Moreover, the use of the term A–algebra means that A is commutative. Frequently our coefficient ring will be a skew field, usually written K or k.

Let R be an A–ring. A family (u_i) of elements of R is **right linearly dependent** over A or **right A–dependent** if there exist $\lambda_i \in A$ almost all (i.e. all but a finite number) but not all zero, such that $\sum u_i\lambda_i = 0$. Otherwise (u_i) is **right A–independent**. Corresponding definitions hold with left instead of right. If such a family is left and right linearly independent (dependent) we call it linearly A–independent (A–dependent). Occasionally we speak of a *set* being linearly dependent or independent; this is to be understood as a family indexed by itself.

As usual, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ stand for the natural numbers, integers, rational numbers, real numbers, complex numbers and the rational quaternions, respec-

tively. *card*(I) or $|I|$ denotes the cardinal number of a set I. If $T \subseteq S$, the complement of T in S is written $S \backslash T$ or, sometimes, $S - T$.

We shall adopt the convention of writting functions on the left of their argument, hence the composition of two functions $A \xrightarrow{f} B \xrightarrow{g} C$ is written $g \circ f$.

All theorems, propositions, lemmas, corollaries, definitions and remarks are numbered consecutively in each section. The end (or absence) of a proof is indicated by ∎.

Lastly, references to the bibliography are by the first three letters of the author's name and the last two digits of the year of publication; thus for instance, Dubrovin [Dub94] refers to a paper of Dubrovin published in 1994.

Introduction

In chapter I we shall give the basic definitions of ring and monoid of fractions and will present the general embedding problem for monoids and rings. We shall mention, briefly, the commutative case as a motivation for finding Ore's condition of embeddability [Ore31]. Originally, Ore treated the particular case of integral domains (cf. corollary I.3.12 on page 28), but these conditions can be re–adapted to obtain the embeddability of any monoid (or even a semigroup) into a group with a prescribed "normal form"(see theorem I.2.5, page 8).

Then, we shall apply Ore's method to skew polynomial rings and shall describe their field of fractions. We shall give several examples of skew polynomial rings where we shall apply the results of the previous sections.

At the end of chapter I, we shall present a family of free algebras of rank two over a given skew field with *countably many non-isomorphic fields of fractions.* The idea of this example is due to Fisher [Fis71], but the proof presented here is original (cf. section I.6 on page 46).

In chapter II we shall present two famous embedding theorems: the Malcev–Neumann and Cohn embedding theorems.

The investigation of geometries, principally by Hilbert [Hil30], with certain incidence and order properties, but lacking others (satisfying "Desargues" but not "Papus") led to the study of totally (fully) ordered division ring. The first example of a centrally infinite division rings was Hilbert's Twisted Laurent se-

ries (see page 45, and also proposition II.2.10 in page 74). The problem of constructing more general types of ordered division rings was begun by Moufang [Mou37], who embedded the group algebra of the free metabelian group of two generators into a division ring and showed that this division ring can be ordered.

Malcev–Neumann's [Mal48, Neu49a] construction of formal power series division rings is also related to Hilbert's example (loc. cit.), with additional motivation coming from the earlier work of Hahn [Hah07] on the embedding of ordered abelian groups into groups of Laurent series.

The main idea of forming Malcev–Neumann formal power series is that one can combine Hilbert's Twisted Laurent series with the usual group ring construction, even with twisted group rings, to get a much bigger class of division rings.

As an application of the Malcev–Neumann embedding we shall embed the free k–algebra over a set X into a division ring, where k is a skew field. Comparing this embedding to the Moufang embedding (loc. cit.) we get another example of a ring with non–isomorphic fields of fractions. As a second application, we shall exhibit an example of a non–Ore ring which can still be embedded in a skew field, showing that the Ore conditions are not necessary to embed a ring in a skew field.

It has been shown by Tamari [Tam53] that the universal enveloping algebra of every *finite dimensional* Lie algebra has the right common multiple condition, hence it is embeddable in a skew field (cf. corollary I.3.12, on page 28). Cohn [Coh61] proved that the universal enveloping algebra of any Lie algebra can be embedded in a skew field. In order to achieve this result, we shall present two theorems due to Cohn [Coh61]: an embedding theorem for a certain class of inverse limit semigroups (theorem II.5.1, page 88) and an embedding theorem for valuated rings satisfying some extra condition (theorem II.6.1, page 92). Following Cohn, we shall reformulate theorem II.6.1 in a suitable way for the

application we shall give in the last section of chapter II: the proof that every Birkhoff–Witt algebra is embeddable in a skew field. We shall use this to show that the universal enveloping algebra of *any* Lie algebra (not necessarily finite dimensional) is embeddable in a skew field; and also to give another proof of the fact that the free algebra $k\langle X\rangle$ (k a commutative field, X a set) is embeddable in a skew field.

In chapter III we shall see a general method [Coh71a, Coh72a, Coh72b, Coh85] of embedding rings in skew fields due to Cohn. This technique is quite general in that it provides a criterion for arbitrary rings to be so embeddable, and also can be used to describe the homomorphisms of rings into skew fields. For a commutative ring such homomorphisms can be completely described in terms of the set of its prime ideals, and in the course of this chapter we shall see that the same description applies to quite general rings.

Let R be a ring. Our basic problem will be to study the possible ways of embedding R into a skew field. Of course there may be no such embedding, and it is more natural to treat the wider problem of finding homomorphisms of R into a skew field.

As we see in corollary I.3.12, page 28, in the Ore case, once we have an R^*–inverting homomorphism, we have achieved the embedding in a field (we even have a unique field of fractions with a prescribed normal form). Assume that K is the field of fractions of an Ore domain R. Then, every element u of K can be written as $a^{-1}b$ ($a, b \in R$). Thus, u is obtained by solving

$$(*) \qquad au - b = 0.$$

But in general, if we have an R^*–inverting homomorphism, we do not necessarily get an embedding in a field; after adjoining the inverses of all non–zero elements of R, there may still be elements without inverses, e.g. $ab^{-1}c + de^{-1}f$ (recall that now we don't have the right multiple condition to "shuffle elements around"),

so we need to perform repeated inversions.

Thus for a non–commutative ring R the R^*–inverting homomorphisms are not very good approximations to homomorphisms into a skew field. Following Cohn, we shall remedy this defect by inverting, instead of elements, a set of square matrices over R (possibly of different orders) and we shall be able to manage with a single inversion if we replace a in $(*)$ by a matrix. Since our aim is to construct skew fields, we shall confine ourselves to square matrices, the only ones that can be inverted over a field (since any field has invariant basis number).

For a commutative ring this gives nothing new, since we can invert any square matrix A simply by adjoining an inverse of *det* A (the determinant of A). But over a non–commutative ring, although a determinant can be defined, it lacks the properties required to achieve an analogous situation to the commutative case, so we expect the inverse of a matrix to give something new. We shall characterize the homomorphisms from R to skew fields by means of the "prime matrix ideal" of R, to be defined in chapter III.

We shall be interested in R–rings that are skew fields, called R–fields. We single out a particular class of R–fields, the epic R–fields, and shall introduce a category having epic R–fields for objects and as morphisms certain equivalence classes of local homomorphisms called specializations. In order to construct epic R–fields we introduce the concepts of singular kernel and universal Σ–inverting ring R_Σ (here Σ is a set of square matrices over R, possibly of different orders). To form the universal Σ–inverting ring R_Σ, essentially means to adjoin to R the entries of the inverses of the matrices of Σ in the most general way possible.

A basic step in the construction of an epic R–field is the description of its elements as components of the solution vector of a matrix equation. Towards this end we shall introduce the Σ–rational closure of R with respect to a ring homomorphism from R to another ring. Then we prove a sort of Cramer's rule for non–commutative rings. **We also prove lemma III.2.3, on page 127,**

which is original. It will give us the exact relation between the universal Σ–inverting ring and the Σ–rational closure. As an application of Cramer's rule and this lemma we shall show how to construct epic R–fields from their singular kernels.

From the above discussion, we know that any epic R–field may be described entirely in terms of matrices over R; we shall also see how to express specializations in terms of the sets of matrices inverted over R: there is a specialization between two epic R–fields iff there is an inclusion relation between their singular kernels. This will give us an equivalence between the category of epic R–fields and specializations and the category whose objects are singular kernels of epic R–fields with inclusion mappings as morphisms.

At this stage, we would like to know when a collection of matrices is a singular kernel, just as we can tell when a collection of elements of R is a prime ideal. In fact we shall be able to characterize singular kernels in much the same way as kernels of R–fields in the commutative case are characterized as prime ideals. To this end we introduce some operations on the set of matrices over R and the notion of a matrix ideal. This corresponds to the concept of an ideal in a commutative ring. Then, we shall define the analogue of a prime ideal: the prime matrix ideal, which has properties corresponding closely to those of prime ideals. Prime matrix ideals can be used to describe homomorphisms of general rings into skew fields, just as prime ideals do in the commutative case.

The crux of chapter III is the following

characterization of prime matrix ideals: prime matrix ideals are the sets of square matrices over R which become singular under a homomorphism into some skew field.

This characterization of prime matrix ideals will be applied to derive criteria for a general ring to be embeddable in a field, or to have a universal field of fractions.

An alternative approach to the method of universal localization was given

by Gerasimov [Ger79, Ger82]. Gerasimov put emphasis in studying homomorphisms of rings into rings (not necessarily skew fields) and characterized all such mappings. His work led to a localization theorem for n–firs. This theorem was proved independently by Malcolmson [Mal84], who simplified some of the proofs of this chapter, cf. [Mal78, Mal80, Mal82, Mal84].

We also mention that Schofield [Sch85] generalized Cohn's method of embedding rings into skew fields and studied finite dimensional representations of a ring over a skew field.

Lastly, in chapter IV, we shall give an outline, without proofs, of Dubrovin's partial solution [Dub94] to the following problem of Malcev: the embedding of the group ring of a left orderable group into a skew field. We remark that Dubrovin needed some extra condition on the left orderable group to obtain the embedding.

CHAPTER I

The General Embedding Problem

In this chapter we shall give the basic definitions of ring and monoid of fractions and will present the general embedding problem for monoids and rings, as defined by P. M. Cohn (cf. e.g. [Coh85]). Let S be a monoid. Let $T \subset S$, $T \neq \emptyset$. The general embedding problem for monoids can be stated as: When does there exist a monoid of fractions of S with denominator set T or better, when does there exist a universal T–inverting monoid of fractions of S with denominator set T? (see page 5); similarly for a ring (see page 21).

We shall see, briefly, the commutative case as a motivation for finding Ore's condition of embeddability [Ore31]. His method gives necessary and sufficient conditions for the embeddability of a ring into a field of fractions with a prescribed "normal form" (see page 8). Originally, Ore treated the particular case of integral domains (cf. corollary I.3.12 on page 28), but these conditions can be re–adapted to get the embeddability of any monoid (or even a semigroup) into a group with a prescribed "normal form"(see theorem I.2.5, page 8).

Then, we shall apply Ore's method to skew polynomial rings and shall de-

scribe their field of fractions. We shall give several examples of skew polynomial rings where we shall apply the results of the previous sections. The last of these examples will give an informal introduction to the topological methods of embedding to be describe in chapter II.

Lastly, we present a family of free algebras of rank two over a given skew field with *countably many non-isomorphic fields of fractions*. The idea of this example is due to Fisher [Fis71], but the proof presented here is original (cf. section I.6 on page 46).

I.1 Fractions

Let S be a set. By an operation on S we mean a function $S \times S \longrightarrow S$. By a semigroup we mean an ordered pair $(S, .)$ where S is a set and "." is an associative operation. Since it is possible to adjoin, formally, a 1 to any semigroup, there's no loss of generality in working with a monoid (a semigroup with 1) instead of considering a semigroup.

By $\mathcal{U}(S)$ we denote the units of a monoid S.

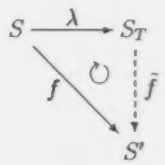
Definition I.1.1 (T–inverting monoid homomorphism) *Let S and S' be monoids and $T \subset S$, $T \neq \emptyset$. A monoid homomorphism $f : S \to S'$ is said to be* **T–inverting** *if $f(T) \subset \mathcal{U}(S')$.*

Definition I.1.2 (monoid and group of fractions) *Let S and S' be monoids and $T \subset S$, $T \neq \emptyset$. Let $f : S \to S'$ be a T–inverting monoid homomorphism. Let U be the submonoid of S' generated by $f(S)$ and $f(T)^{-1} := \{f(t)^{-1} : t \in T\}$. If f is an embedding (i.e., f is injective), then the pair (U, f) is called a* **monoid of fractions** *of S with* **denominator set** *T. When $T = S$, we call such a pair a* **group of fractions** *of S.*

Definition I.1.3 (Universal T–inverting monoid and universal group) *Let S be a monoid and $T \subset S$, $T \neq \emptyset$. By a* **Universal T–inverting monoid**

of S with denominator set T we understand a pair (S_T, λ) consisting of a monoid S_T and a T–inverting monoid homomorphism $\lambda: S \longrightarrow S_T$ with the following universal property: given any monoid S' and any T–inverting homomorphism $f: S \longrightarrow S'$, there exists a unique monoid homomorphism $\tilde{f}: S_T \longrightarrow S'$ such that $f = \tilde{f} \circ \lambda$. When $T = S$, then S_T is a group, written $\mathcal{G}(S)$ and called the universal group of S.

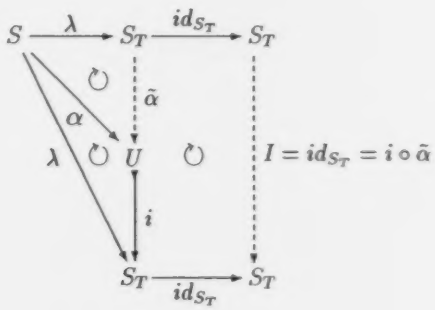
(I.1)



The existence and uniqueness of (S_T, λ) will be established in remark I.1.5 (see page 4), but first we give an element–wise characterization of S_T.

Proposition I.1.4 *Let S be a monoid and $T \subset S$, $T \neq \emptyset$. Let (S_T, λ) be a universal T–inverting monoid of S. Let U be the submonoid of S_T generated by $\lambda(S) \bigcup \lambda(T)^{-1}$. Then, $U = S_T$.*

Proof. Since $\lambda(S) \subset U$, we can define $\alpha: S \longrightarrow U$ by $\alpha(s) = \lambda(s)$, for all $s \in S$, i.e., α is the corestriction of λ to U. Note that α is a monoid homomorphism, since λ is, and α is T–inverting, since U contains $\lambda(T)^{-1}$, by definition of U.



Consider the T–inverting homomorphism $\alpha: S \longrightarrow U$. By the universal property of (S_T, λ), there exists a unique monoid homomorphism $\tilde{\alpha}: S_T \longrightarrow U$ such that $\alpha = \tilde{\alpha} \circ \lambda$. Let $i: U \hookrightarrow S_T$ be the inclusion map. Consider the T–inverting homomorphism $\lambda: S \longrightarrow S_T$. By the universal property of (S_T, λ), there exists a unique monoid homomorphism $I: S_T \longrightarrow S_T$, such that $\lambda = I \circ \lambda$. Since the identity function on S_T, $id/_{S_T} : S_T \longrightarrow S_T$, verifies the same conditions as I does, we have that $I = id/_{S_T}$, from the uniqueness of I. It follows simirlarly that $i \circ \tilde{\alpha} = I = id/_{S_T}$. Similarly, $\tilde{\alpha} \circ i = id/_U$ and hence both $\tilde{\alpha}$ and i are isomorphisms. ∎

Remark I.1.5 *(S_T, λ) may be constructed by considering a monoid presentation of S, in terms of generators and defining relations. For each $t \in T$, adjoin, formally, an element t' (not belonging to T), with additional relation $tt' = t't = 1$. Define $\lambda: S \longrightarrow S_T$, by assigning to each element in S the corresponding element in the presentation. Then, $\lambda(t)$ is invertible, the inverse being t'. Given a T–inverting monoid homomorphism $f: S \longrightarrow S'$, where S' is another monoid, define $\bar{f}: S_T \longrightarrow S'$ by mapping $\lambda(s)$ to $f(s)$ and s' to $f(s)^{-1}$ $(s \in S)$, which exists in S' by assumption. Any relation in S_T must be a consequence of relations in S and relations expressing that s' is the inverse of $\lambda(s)$. Since all these relations still hold in S', so $\bar{f}$ is well defined and it is clearly a homomorphism, by construction. It is unique because its values are prescribed on $\lambda(S)$ and $\lambda(S)^{-1}$, which generate S_T by proposition I.1.4.*

Proposition I.1.6 *Let S, S', S'' be monoids. Let $T \subset S$, $T \neq \emptyset$ and $T' \subset S'$, $T' \neq \emptyset$. Then, for any monoid homomorphism $f: S \longrightarrow S'$, such that $f(T) \subset T'$ and any T'–inverting monoid homomorphism $g: S' \longrightarrow S''$, there exists a unique monoid homomorphism $F: S_T \longrightarrow S''$, such that $F \circ \lambda = g \circ f$.*

Proof. Let (S_T, λ) be the universal T–inverting monoid on S. Consider $g \circ f : S \longrightarrow S''$. Since $f(T) \subset T'$, by assumption, and since $g(T') \subset U(S'')$ (because g is T'–inverting), then $g \circ f(T) \subset U(S'')$, i.e., $g \circ f$ is T–inverting, so, by the universal property of (S_T, λ), there exists a unique monoid homomorphism $F : S_T \longrightarrow S''$ such that the above diagram commute. Any other monoid homomorphism from $S_T \longrightarrow S''$ that makes the above diagram commute must be equal to F because $g \circ f$ is T–inverting and by the uniqueness in the universal property of (S_T, λ). ∎

I.2 The general embedding problem for monoids

Let S be a monoid. Let $T \subset S$, $T \neq \emptyset$. **The general embedding problem for monoids** can be stated as: When does there exist a monoid of fractions of S with denominator set T, or better, when does there exist a universal T–inverting monoid of fractions of S with denominator set T?.

Definition I.2.1 (Cancellative subset of a monoid) *Let S be a monoid. Let $T \subset S$, $T \neq \emptyset$. We say that T is a **cancellative subset** of S when the following condition holds:*

(I.2) $\quad \forall s,\ s' \in S,\ t \in T :$ *if $st = s't$ or $ts = ts'$, then $s = s'$.*

In this case, we also say that S admits ***cancellation by*** $\mathbf{T}$. *When $T = S$, we call S a* ***cancellation monoid***.

Proposition I.2.2 *Let S be a monoid, $T \subset S$, $T \neq \emptyset$. Let (U, f) be a monoid of fractions of S with denominator set T. A necessary condition for f to be injective is that T be a cancellative subset of S.*

Proof. If $st = s't$ (the case $ts = ts'$ is similar and we omit it) then:

$$\begin{aligned} \lambda(st) &= \lambda(s't), \\ \lambda(s)\lambda(t) &= \lambda(s')\lambda(t), \end{aligned}$$

Cancelling with $\lambda(t)^{-1}$, we get:

$$\begin{aligned} \lambda(s) &= \lambda(s') \\ s &= s' \end{aligned}$$

since we assume that λ is injective. So, (I.2) holds. ∎

We shall see a case where the general embedding problem can always be solved, namely, when we localize by an Ore set (see definition I.2.4, page 8). In this case, a monoid of fractions is easy to construct and has a nice "normal form", in fact, it is unique up to monoid isomorphism (see proposition I.2.7, page 15). But before introducing Ore's conditions, let us look at the commutative, where a monoid of fractions exists if and only if we localize by a cancellative subset, i.e., condition (I.2) is not only necessary, but also sufficient to solve the general embedding problem for a commutative monoid.

Proposition I.2.3 (Localization for a commutative monoid) *Let S be a commutative monoid. Let $T \subset S$, $T \neq \emptyset$. Assume that S admits cancellation by T. Then, there exists a monoid U and a monoid homomorphism $\lambda : S \longrightarrow U$, such that (U, λ) is a monoid of fractions of S with denominator set T.*

Proof. Consider the Cartesian product $\Delta := S \times T$. Define a mapping

$$\text{(I.3)} \qquad \begin{array}{rcl} . : \Delta \times \Delta & \longrightarrow & \Delta \\ ((s_1,t_1),(s_2,t_2)) & \mapsto & (s_1,t_1).(s_2,t_2) := (s_1s_2, t_1t_2). \end{array}$$

Consider the relation "$\sim$" on Δ given by

$$\text{(I.4)} \qquad (s_1,t_1) \sim (s_2,t_2) \longleftrightarrow s_1t_2 = s_2t_1.$$

The relation "$\sim$" is, clearly, reflexive and symmetric. We show it is transitive. If $(s_1,t_1) \sim (s_2,t_2)$ and $(s_2,t_2) \sim (s_3,t_3)$ then, by (I.4), $s_1t_2 = s_2t_1$ and $s_2t_3 = s_3t_2$. So,

$$\begin{array}{rcl} s_1t_2t_3 & = & s_2t_1t_3 \\ s_2t_3t_1 & = & s_3t_2t_1. \end{array}$$

Then, since S is commutative and admits cancellation by T,

$$s_1t_3 = s_3t_1$$

Hence, $(s_1,t_1) \sim (s_3,t_3)$. Then, "$\sim$" is an equivalence relation on Δ. We now show that "$\sim$" is compatible with the composition law (I.3) on Δ. Assume, $(s_1,t_1) \sim (s_2,t_2)$ and $(s_3,t_3) \sim (s_4,t_4)$. We prove that $(s_1,t_1).(s_3,t_3) \sim (s_2,t_2).(s_4,t_4)$. Since, $s_1t_2 = s_2t_1$ and $s_3t_4 = s_4t_3$, by assumption, then $s_1t_2s_3t_4 = s_2t_1s_4t_3$, so, $s_1s_3t_2t_4 = s_2s_4t_1t_3 \longleftrightarrow (s_1s_3, t_1t_3) \sim (s_2s_4, t_2t_4) \longleftrightarrow (s_1,t_1).(s_3,t_3) \sim (s_2,t_2).(s_4,t_4)$. Hence,"$\sim$" is compatible with (I.3). We may form the quotient monoid $\Delta/\sim$. Denote by $[(s,t)]$ the equivalence class of (s,t). Define $U := (\Delta/\sim, .)$ where "." is the induced composition on $\Delta/\sim$ by (I.3). Since S is commutative, then, U is also commutative. Define $\lambda : S \longrightarrow U$ by $s \mapsto [(s,1)]$. Then, λ is injective (since, $[(s_1,1)] = [(s_2,1)] \longrightarrow s_1 = s_2$) and is,

clearly, a homomorphism. We show (U, λ) is a monoid of fractions of S with denominator set T. Note that $[(t,1)]^{-1} = [(1,t)]$, since $(t,1).(1,t) = (t,t) \sim (1,1)$, so λ is T–inverting. From $[(s,t)] = [(s,1)].[(1,t)]$, it follows that U is generated by $\lambda(S)$ and $\lambda(T)^{-1}$. So, (U, λ) is a monoid of fractions of S with denominator set T. By, proposition I.2.7, uniqueness of the monoid of fractions for a right Ore set, (see page 15), it will follow that any monoid of fractions is isomorphic to S_T. ∎

Let S be a monoid. Let $T \subset S$ *and* $T \neq \emptyset$. Let (S_T, λ) be the universal T–inverting monoid of S with denominator set T. Assume that λ is injective (hence, (S_T, λ) is a monoid of fractions). Then we can identify $S \cong \lambda(S)$. **Assume that every element of S_T can be written in the "normal form"** st^{-1} $(s \in S,\ t \in T)$. In this case, we write $S_T = ST^{-1}$. Hence, in particular, if $t \in T,\ s \in S$, then $t^{-1}s$ must have this form, say $t^{-1}s = s_1 t_1^{-1}$, for some $t_1 \in T,\ s_1 \in S$ and we find $st_1 = ts_1$. We combine this condition with the necessary condition I.2 in the following definition.

Definition I.2.4 (Ore's conditions for a monoid) *Let S be a monoid. Let T be a submonoid of S. We say that T is a* ***right Ore set*** *in S if and only if*

(I.5) $\quad \forall s,\ s' \in S,\ t \in T: \quad$ *if* $st = s't$ *or* $ts = ts'$, *then* $s = s'$

(I.6) $\quad \forall s \in S,\ t \in T: \quad sT \cap tS \neq \emptyset.$

Theorem I.2.5 (Ore's embedding for a monoid) *Let S be a monoid. Let T be a right Ore set in S. Let (S_T, λ) be the universal T–inverting monoid of S. Then, (S_T, λ) is a monoid of fractions and every element of S_T has the form st^{-1} $(s \in S,\ t \in T)$. Conversely, when $S_T = ST^{-1}$ and λ is an embedding, then T is a right Ore set in S.*

Proof.

Let $\Delta := S \times T$. Define a relation "$\sim$" on Δ by

(I.7) $(s_1, t_1) \sim (s_2, t_2) \longleftrightarrow \exists u_1, u_2 \in S : t_1 u_2 = t_2 u_1 \in T,\ s_1 u_2 = s_2 u_1.$

Assume that $(s_1, t_1) \sim (s_2, t_2)$. Then, by (I.7), there exist $u_1, u_2 \in S$, such that,

(I.8) $$t_1 u_2 = t_2 u_1 \in T$$

(I.9) $$s_1 u_2 = s_2 u_1.$$

Claim:

(I.10) $$\textit{If } \exists\, s, s' \in S : \ t_1 s = t_2 s' \in T$$

$$\textit{then } s_1 s = s_2 s'$$

Indeed, by (I.6), there exists $\tilde{s} \in S$, $\tilde{t} \in T$, such that,

(I.11) $$(t_1 u_2)\tilde{s} = (t_1 s)\tilde{t}$$

(I.12) $$(t_2 u_1)\tilde{s} = (t_2 s')\tilde{t}, \textit{ using } (I.8) \textit{ and } (I.10)$$

(I.13) $$u_2 \tilde{s} = s\tilde{t}, \textit{ by cancelling } t_1 \textit{ in } (I.11)$$

(I.14) $$u_1 \tilde{s} = s'\tilde{t}, \textit{ by cancelling } t_2 \textit{ in } (I.12)$$

Now, consider $s_1 s\tilde{t}$,

$$s_1 s\tilde{t} = s_1 u_2 \tilde{s}, \textit{ by multiplying with } s_1 \textit{ in } (I.13)$$

$$s_1 u_2 \tilde{s} = s_2 u_1 \tilde{s}, \textit{ by } (I.9)$$

$$s_2 u_1 \tilde{s} = s_2 s'\tilde{t}, \textit{ by } (I.14)$$

So, $s_1 s\tilde{t} = s_2 s'\tilde{t}$, hence, $s_1 s = s_2 s'$ and the claim holds.

We show that "$\sim$" is transitive. Assume that $(s_1, t_1) \sim (s_2, t_2)$ and $(s_2, t_2) \sim (s_3, t_3)$. Then, by definition of "$\sim$" (see (I.7)), there exist $u_1, u_2, v_2, v_3 \in S$, such that,

$$\begin{aligned} s_1u_2 &= s_2u_1 \\ t_1u_2 &= t_2u_1 \in T \end{aligned} \tag{I.15}$$

$$\begin{aligned} s_2v_3 &= s_3v_2 \\ t_2v_3 &= t_3v_2 \in T. \end{aligned} \tag{I.16}$$

Since $t_2u_1 \in T$, then by (I.6),

$$(t_2u_1)S \cap t_2v_3T \neq \emptyset, \tag{I.17}$$

so, there exist $s' \in S$, $t' \in T$, such that,

$$t_2u_1s' = t_2v_3t'. \tag{I.18}$$

Note that since $t_2v_3 \in T$, by (I.16), then $t_2v_3t' \in T$, since $t' \in T$ and T is a monoid; so, by (I.18),

$$t_2u_1s' \in T. \tag{I.19}$$

Consider t_1u_2s',

$$\begin{aligned} t_1u_2s' &= t_2u_1s', \textit{ by multiplying with } s' \textit{ in } (I.15) \\ t_2u_1s' &= t_2v_3t', \textit{ by } (I.18) \\ t_2v_3t' &= t_3v_2t', \textit{ by } (I.16), \end{aligned} \tag{I.20}$$

then, $t_1u_2s' = t_3v_2t' \in T$, by (I.19) and (I.20). So, by the above claim,

$$s_1u_2s' = s_3v_2t',$$

and, hence, $(s_1,t_1) \sim (s_3,t_3)$, by definition of "$\sim$".

$\therefore$ "$\sim$" is an equivalence relation on Δ.

We define a multiplication on Δ as follows: given $(s_1,t_1),(s_2,t_2) \in \Delta$, we can find, by (I.6), $u_1 \in T, u_2 \in S$, such that

(I.21) $$t_1u_2 = s_2u_1.$$

Now, define

(I.22) $$(s_1,t_1).(s_2,t_2) := (s_1u_2, t_2u_1);$$

since $t_2u_1 \in T$, this defines an element of Δ.

First, note that (I.22) does not depend on the particular u_1 and u_2 chosen. Indeed, if $u_1' \in T, u_2' \in S$ are such that

(I.23) $$t_1u_2' = s_2u_1',$$

then, by (I.6), there exist $x \in T, x' \in S$, such that,

(I.24) $$u_1x = u_1'x' \in T, \text{ since } u_1, x \in T,$$

whence

$$t_2u_1x = t_2u_1'x', \text{ by multiplying (I.24) with } t_2 \tag{I.25}$$

$$s_2u_1x = s_2u_1'x', \text{ by multiplying (I.24) with } s_2$$

$$t_1u_2x = t_1u_2'x', \text{ replacing with (I.21) and (I.23)}$$

$$u_2x = u_2'x', \text{ cancelling } t_1$$

$$s_1u_2x = s_1u_2'x', \text{ multiplying by } s_1. \tag{I.26}$$

Hence, from (I.26) and (I.25)

$$(s_1u_2, t_2u_1) = (s_1u_2', t_2u_1'). \tag{I.27}$$

So, the definition (I.22) does not depend on the particular u_1 and u_2 chosen.

Let us use the suggestive notation $s/t := (s,t)$.

We show that "$\sim$" is compatible with the composition law (I.22). Let $s_1/t_1 = s_1'/t_1'$ and $s_2/t_2 = s_2'/t_2'$. By (I.6), there exist u, u', such that,

$$t_1u = t_1'u' \in T, \tag{I.28}$$

whence, by the above claim,

$$s_1u = s_1'u'; \tag{I.29}$$

next, there exist $v, v' \in T$ and $c, c' \in S$, such that,

$$s_2v = t_1uc \tag{I.30}$$

$$s_2'v' = t_1'u'c'. \tag{I.31}$$

Then, by definition of ".",

$$s_1/t_1.s_2/t_2 = s_1uc/t_2v \tag{I.32}$$

$$s'_1/t'_1.s'_2/t'_2 = s'_1u'c'/t'_2v. \tag{I.33}$$

By (I.6), there exist x, x', such that,

$$t_2vx = t'_2v'x' \in T, \tag{I.34}$$

then, by the above claim,

$$s_2vx = s'_2v'x';$$

whence

$$t_1ucx = t'_1u'c'x', \text{ by } (I.30) \text{ and } (I.31) \tag{I.35}$$

$$cx = c'x', \text{ by } (I.28)$$

$$s_1ucx = s'_1u'c'x', \text{ by } (I.29). \tag{I.36}$$

Then, by (I.36) and (I.34)

$$s_1uc/t_2v = s'_1u'c'/t'_2v',$$

hence, by (I.32) and (I.33),

$$s_1/t_1.s_2/t_2 = s'_1/t'_1.s'_2/t'_2,$$

and this shows that "$\sim$" is compatible with ".".

Now, we are going to write s/t to mean the equivalence class of (s,t) in Δ.

Define $S_T := \Delta/\sim$ with the induced operation by ".". Let $s_1/t_1, s_2/t_2, s_3/t_3 \in S_T$; by (I.6), let $d \in S, v \in T$, be such that $s_2v = t_1d$ and let $e \in S, w \in T$,

such that $s_3w = t_2ve$, then

$$\begin{aligned}(s_1/t_1.s_2/t_2).s_3/t_3 &= s_1d/t_2v.s_3/t_3\\ &= s_1de/t_3w\end{aligned}$$

$$\begin{aligned}s_1/t_1.(s_2/t_2.s_3/t_3) &= s_1/t_1.(s_2ve/t_3w)\\ &= s_1de/t_3w,\end{aligned}$$

whence, "." is associative.

Note that $s/t\ .\ 1/1 = 1/1\ .\ s/t = s/t$, so, $1/1$ is the unity; and for all $t \in T$, $1/t\ .\ t/1 = t/1\ .\ 1/t = 1/1$, so, $t/1$ is invertible, for all $t \in T$.

Define a mapping $\lambda : S \longrightarrow S_T$ given by $s \mapsto s/1$. It is routine to check that it is a T–inverting monoid homomorphism, and it is injective because if $s_1/1 \sim s_2/1$, then, by (I.7), $s_1u_2 = s_2u_1$, *for some* $u_1 = u_2 \in T$, whence $s_1 = s_2$, by (I.5).

Given a T–inverting monoid homomorphism $f : S \longrightarrow S'$, where S' is another monoid, define $\tilde{f} : S_T \longrightarrow S'$ by mapping $\lambda(s)$ to $f(s)$ and $\lambda(t)^{-1}$ to $f(t)^{-1}$ $(t \in T, s \in S)$, which exists in S' by assumption. Any relation in S_T is a consequence of relations in S and relations expressing that $1/t$ is the inverse of $\lambda(t) = t/1$. Since all these relations still hold in S' (since f is T–inverting), $\tilde{f}$ is well defined and it is clearly a homomorphism, by construction. It is unique because its values are prescribed on $\lambda(S)$ and $\lambda(S)^{-1}$, which generate S_T since $S_T = ST^{-1}$ (because $s/t = s/1.1/t$. So, (S_T, λ) is the universal T–inverting monoid on S.

Conversely, when S is embedded in S_T, then by proposition I.2.2, (I.5) holds, and since $S_T = ST^{-1}$, then (I.6) holds, hence, T is a right Ore set on S. ∎

We note that any finite set of elements of S_T may be brought to a "common denominator", which is a right multiple of the denominators of the given

elements. We formalize this claim in the following:

Lemma I.2.6 (Common denominator lemma for a monoid) *Let S be a monoid, $T \subset S, T \neq \emptyset$. Assume that T is a right Ore set. Let $\lambda : S \longrightarrow S_T$ be the universal T–inverting monoid homomorphism. Let $x_1, \ldots, x_n \in S_T$, where $x_i = s_i t_i^{-1}, s_i \in S, t_i \in T, 1 \leq i \leq n$.*

Then, there exist $t \in T$ ("a common denominator") and $s_i' \in S, 1 \leq i \leq n$, such that, $x_i = s_i' t^{-1}, 1 \leq i \leq n$.

Proof. By induction on n. By theorem I.2.5, λ is injective and $S_T = ST^{-1}$. Assume $n = 2$. Let $x_1, x_2 \in S_T$. Then, $x_1 = s_1 t_1^{-1}$ and $x_2 = s_2 t_2^{-1}$. By (I.6), assume

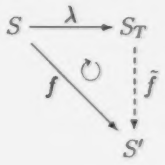
$$t_1 u_2 \quad = \quad t_2 u_1, \text{ where } u_2 \in T, u_1 \in S;$$

hence $t := t_1 u_2 = t_2 u_1 \in T$ and $x_1 = s_1 u_2 (t_1 u_2)^{-1}$, $x_2 = s_2 u_1 (t_2 u_1)^{-1}$. Hence, the case $n = 2$ holds.

When we have $n \geq 2$ elements $x_1, \ldots, x_n$, we first bring $x_2 \ldots, x_n$ to a common denominator t' and then bring x_1, t' to a common denominator t. Then, t is the desired common denominatro of $x_1, \ldots, x_n$, and a right multiple of the original denominators. ∎

Proposition I.2.7 (Uniqueness of the monoid of fractions) *Let S be a monoid and T be a right Ore set on S. Then, any monoid of fractions of S with denominator set T is monoid–isomorphic to S_T.*

Proof. Let (S_T, λ) be the universal T–inverting monoid on S. Let S' be a monoid of fractions of S with denominator set T, with T–inverting homomorphism $f : S \longrightarrow S'$. By the universal property of (S_T, λ), there exists a (unique) monoid homomorphism $\tilde{f} : S_T \longrightarrow S'$, such that,



We know that $\tilde{f}$ is a monoid homomorphism. We show that $\tilde{f}$ is an isomorphism. First, we check injectivity. Let $c_1, c_2 \in S_T$, then, by lemma I.2.6, assume

$$c_1 = a_1 b^{-1}, c_2 = a_2 b^{-1}, \tag{I.37}$$

where $b \in T, a_i \in S$. Since, λ is injective (because T is right Ore, see theorem I.2.5, page 8), we identify $\lambda(s) = s, \forall s \in S$. So, we assume that $S \subset S_T$. Assume

$$\tilde{f}(c_1) = \tilde{f}(c_2). \tag{I.38}$$

Then[1],

$$\begin{aligned} f(a_1) &= \tilde{f}(a_1) \\ &= \tilde{f}(a_1)\tilde{f}(b^{-1})\tilde{f}(b) \\ &= \tilde{f}(a_1 b^{-1})\tilde{f}(b) \\ &= \tilde{f}(c_1)\tilde{f}(b) \\ &= \tilde{f}(c_2)\tilde{f}(b), \text{ by } (I.38) \\ &= \tilde{f}(a_2 b^{-1})\tilde{f}(b) \\ &= \tilde{f}(a_2)\tilde{f}(b^{-1})\tilde{f}(b) \\ &= \tilde{f}(a_2) \\ &= f(a_2). \end{aligned}$$

Since f is injective (because S' is a monoid of fractions), then

$$a_1 = a_2,$$

hence, by (I.37),

$$c_1 = c_2,$$

$\therefore \tilde{f}$ is injective.

Since f is injective, we identify $f(s) = s, \forall s \in S$. So, we assume that $S \subset S'$. Since $\tilde{f}$ is injective and our homomorphisms preserve 1, we can identify the inverse of t in S_T with the inverse of t in S'.

To check that $\tilde{f}$ is surjective, recall that by definition of monoid of fractions (see definition I.1.2, page 2), S' is generated, as a monoid, by $f(S)$ and $f(T)^{-1}$.

[1]Recall that all our homomorphisms preserve 1.

So, let $s' \in S'$, then we can write

$$s' = \prod_{i=1}^{n} x_i, \text{ where } x_i \in f(S) \text{ or } x_i \in f(T)^{-1}.$$

If $x_i \in f(S)$, assume $x_i = f(s_i)$, for some $s_i \in S$.

If $x_i \in f(T)^{-1}$, assume $x_i = {t_i}^{-1}$, for some ${t_i}^{-1} \in f(T)^{-1}$ $(= \lambda(T)^{-1}$, by above comment).

Define $x := \prod_{i=1}^{n} r_i$, *where either* $r_i = s_i$, *if* $x_i \in f(S)$ *or* $r_i = t_i^{-1}$, *if* $x_i \in f(T)^{-1}$. Then,

$$\begin{aligned} \tilde{f}(x) &= \tilde{f}(\prod_{i=1}^{n} r_i) \\ &= \prod_{i=1}^{n} \tilde{f}(r_i) \\ &= \prod_{i=1}^{n} x_i, \text{ by definition of } r_i, \end{aligned}$$

$\therefore \tilde{f}$ is surjective. ∎

The following corollary will be used in the proof of theorem II.5.1, (see page 88) where we shall extend Ore's embedding theorem for monoids (theorem I.2.5, page 8) to the inverse limit of semigroups.

Corollary I.2.8 *Let S be a cancellation semigroup, i.e. the following condition holds:*

(I.39) $\quad \forall s,\ s',\ t \in S:$ *if* $st = s't$ *or* $ts = ts'$, *then* $s = s'$.

Moreover, assume that S satisfies the right multiple condition

(I.40) $\quad sS \cap tS \neq \emptyset$ *for all* $s, t \in S$.

Then, S has a unique group of right quotients, i.e. there exists a unique group G such that S is a subsemigroup of G and every element of G has the form st^{-1} $(s, t \in S)$; thus

$$G = SS^{-1}.$$

Moreover, any semigroup homomorphism ϕ of S into a group H can be extended to a unique homomorphism $\overline{\phi}$ of G into H.

Proof. As we pointed out at the beginning of section I.1, S can be embedded in a monoid. So, without loss of generality, we can assume that S is a monoid. Now, the existence of a group G of right quotients follows by putting $S = T$ in theorem I.2.5 (see page 8) and the fact that a monoid for which every element has an inverse is a group. The uniqueness of G follows from proposition I.2.7.

The "moreover" part follows from proposition I.1.6 (see page 4) for $T = S$, $S' = S'' = H$, $g = id_H$, $f = \phi$ and noting that any semigroup homomorphism from S into a group is S–inverting. ∎

I.3 The general embedding problem for rings

We can apply the definitions and constructions given so far to a ring, more specifically, to the multiplicative monoid of a ring. To avoid a total collapse, we shall consider subsets T of $R^\times$ as denominator sets, where $R^\times$ are the non–zero elements of R, since we don't want to invert 0 and get the zero–ring. Given a ring R, we denote by $\mathcal{U}(R)$ the units of R.

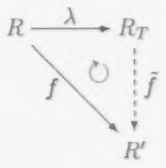
Definition I.3.1 (T–inverting ring homomorphism) *Let R and R' be rings and $T \subset R^\times$, $T \neq \emptyset$. A ring homomorphism $f : R \to R'$ is said to be* **T–inverting** *if $f(T) \subset \mathcal{U}(R')$.*

Definition I.3.2 (Ring of fractions) *Let R and R' be rings and $T \subset R$, $T \neq \emptyset$. Let $f : R \to R'$ be a T–inverting ring homomorphism. Let K be the subring of R' generated by $f(R)$ and $f(T)^{-1} := \{f(t)^{-1} : t \in T\}$. If f is an embedding*

(i.e., f is injective), then the pair (K, f) is called a ***ring of fractions*** *of R with denominator set T.*

Definition I.3.3 (Universal T–inverting ring) *Let R be a ring and $T \subset R$, $T \neq \emptyset$. By a* ***Universal T–inverting ring*** *of R with denominator set T we understand a ring R_T with a T–inverting ring homomorphism $\lambda\colon R \longrightarrow R_T$ with the following universal property: given any ring R' and any T–inverting homomorphism $f\colon R \longrightarrow R'$, there exists a unique ring homomorphism $\tilde{f}\colon R_T \longrightarrow R'$ such that $f = \tilde{f} \circ \lambda$.*

(I.41)



The existence and uniqueness of (R_T, λ) is established similarly as in the monoid case (using proposition I.3.4 below, c.f. remark I.1.5, page 4) and will be omitted.

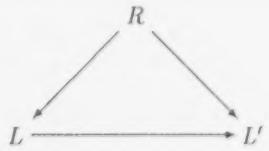
Proposition I.3.4 *Let R be a ring and $T \subset R$, $T \neq \emptyset$. Let (R_T, λ) be a universal T–inverting ring of R. Let U be the subring of R_T generated by $\lambda(R) \bigcup \lambda(T)^{-1}$. Then, $U = R_T$.*

Proof. The proof of this proposition is completely similar to that given in the monoid case in proposition I.1.4 (see page 3) and will be omitted. ∎

The ring R_T constructed above, together with the canonical homomorphism $\lambda\colon R \longrightarrow R_T$ is also called **the localization of R at the set T**. To study R_T we shall do some simplifying assumptions in theorem I.3.8 (see page 23) due to O. Ore [Ore31].

Definition I.3.5 (R–ring) *Let R be a ring. Then a ring L is an R–ring if there exists a ring homomorphism $R \longrightarrow L$.*

For fixed R, the R–rings form a category having as **morphisms** the ring homomorphisms $L \longrightarrow L'$ such that the triangle shown is commutative.



Since our main interest is to embed rings in fields, we shall not develop the general theory of rings of fractions further (for an encyclopedic study see [Str75]) and we shall restrict our attention to fields of fractions, which we now define.

Definition I.3.6 (Field of fractions of a ring) *Let R be a ring. By a **field of fractions** of R we understand a field K together with an embedding $R \overset{\lambda}{\hookrightarrow} K$ such that K is generated as a field by $\lambda(R)$.*

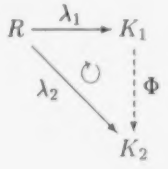
Let R be a ring. **The general embedding problem for rings** can be stated as: When does there exist a field of fractions of R, or better, when does there exist a universal epic field of fractions of R? (for the definition of universal epic field of fractions of a ring see page 118).

For the sake of completeness, we shall mention, without proof, the well known commutative case first. The proof can be found in any standard algebra book (cf. [Hun89], page 142). Actually, the following proposition will follow from Ore's embedding theorem for rings I.3.8, (see page 23).

Proposition I.3.7 *Let R be a commutative ring.*

Existence *A field of fractions (K, λ) exists if and only if R is an integral domain*

Uniqueness *When a field of fractions exists, it is unique up to isomorphisms, i.e., given any fields of fractions of R, $R \overset{\lambda_1}{\hookrightarrow} K_1$, $R \overset{\lambda_2}{\hookrightarrow} K_2$, there exists a ring isomorphism $\Phi\colon K_1 \longrightarrow K_2$ such that*



"Normal form" *Each element of the ring of fractions can be written in the form $a/t := at^{-1}$, where a, $0 \neq t \in R$ and $a/t = a'/t'$ iff $at't'' = a'tt''$, for some $t'' \in T$.* ∎

The normal form referred above is really a normal form only in those rings where there is a canonical representative of each equivalence class, such as $\mathbb{Z}$ or $K[x]$ (K a commutative field) and more general, in UFD's.

In theorem I.2.5, on page 8, we constructed the universal monoid of fraction S_T, where S is a monoid and T is a right Ore set. This construction can be carried out for a ring as well. But for the result to be of use, we must have a means of comparing expressions in R_T and these will require further hypotheses to be imposed (Ore's conditions for a ring). This will be done in theorem I.3.8 below.

For a general treatment it is not enough to invert elements, it is necessary to invert matrices rather than just elements. This program will be carried out in chapter III.

As we outlined in the monoid case, Ore's fruitful idea is to look at the case where all the elements of R_T can be written as simple fractions $(\lambda(a))(\lambda(t))^{-1}$, $a \in R$, $t \in T$. If this is to be possible, we must in particular be able to express $(\lambda(t)^{-1})(\lambda(a))$ in this form: $(\lambda(t)^{-1}(\lambda(a)) = (\lambda(a_1))(\lambda(t_1))^{-1}$, hence, we obtain

$$\lambda(at_1) = \lambda(a_1 t)$$

and this provides a clue to the condition needed. Of course, if every element is to be expressed as a fraction with denominator from the set T, we must also assume T to be multiplicative and to contain 1, i.e. to be a monoid.

Theorem I.3.8 (Ore's theorem for a ring) *Let R be a ring. Let T be a multiplicative monoid of R such that*

O.1

$$aT \cap tR \neq \emptyset \text{ for all } a \in R,\ t \in T. \tag{I.42}$$

O.2

(I.43)

$$\text{for each } a \in R,\ t \in T,\ \text{if } ta = 0,\ \text{then } at' = 0 \text{ for some } t' \in T.$$

Then, the elements of the universal T-inverting ring R_T can be constructed as fractions a/t, where

$$\text{(I.44) } a/t = a'/t' \longleftrightarrow au = a'u' \text{ and } tu = t'u' \in T,\ \text{for some } u,\ u' \in R.$$

Moreover, the kernel of the natural homomorphism $\lambda\colon R \longrightarrow R_T$ is

$$\ker \lambda = \{a \in R / at = 0 \text{ for some } t \in T\}.$$

The proof of the above theorem will be given after we introduce some definitions and prove the common denominator lemma for rings.

Condition (I.42) is called the **right Ore condition for rings**. A multiplicative submonoid T of R satisfying (I.42) is called a **right Ore set of a ring**; if T also satisfies (I.43), it is called **right reversible** or also a **right denominator set for a ring**. By theorem I.3.8, such a set allows the construction of **right fractions** $a/t = (\lambda(a))(\lambda(t)^{-1})$. They must be carefully distinguished from **left**

fractions $(\lambda(t)^{-1})(\lambda(a))$ due to the lack of commutativity. By symmetry we have the notion of a **(reversible) left Ore set for a ring**, which allows us to construct all the elements of R_T as left fractions.

The following property of fractions is very useful.

Lemma I.3.9 (Common denominator lemma for a ring) *Let R be a ring with a reversible right Ore set T and universal T-inverting ring R_T. Then, any finite set in R_T can be brought to a common denominator.*

Proof: We shall use induction on the number of elements. Let $a_i/t_i \in R_T$ be given, $i = 1, \ldots, n$. For $n = 1$ there is nothing to prove; so by induction we may assume these fractions to be in the form $a_1/t_1, a_2/t, \ldots, t_n/t$. By (I.42) there exist $t \in T$, $c \in R$ such that $tc = t_1 t = u \in T$, hence the fractions can be written $a_1 t/u, a_2 c/u, \ldots, a_n c/u$. ∎

Proof of theorem I.3.8: We define a relation on $\Delta := R \times T$ by writting

(I.45)

$(a,t) \sim (a',t') \longleftrightarrow$ *there exist* $u, u' \in R$ *such that* $au = a'u', tu = t'u' \in T$.

We claim that this is an equivalence relation (this is similar to the proof of theorem I.2.5, see page 8, but here we shall give a shorter proof because we can use the addition of R). Clearly, it is reflexive and symmetric. To prove transitivity, let $(a,t) \sim (a',t') \sim (a'',t'')$; say $au = a'u', tu = t'u' \in T, a'v = a''v', t'v = t''v' \in T$. By (I.42), there exist $z \in T, z' \in R$ such that $t'u'z = t'vz'$, hence $t'u'z \in T$ (since T is multiplicative closed) and moreover, $t'(u'z - vz') = 0$, therefore by (I.43), there exists $w \in T$ such that $u'zw = vz'w$. Now, we have $auzw = a'u'zw = a'vz'w = a''v'z'w$, $tuzw = t'u'zw = t'vz'w = t''v'z'w$, and this lies in T because $t'u'z \in T$ and $t \in T$. Thus, $(a,t) \sim (a'',t'')$.

We then have an equivalence on $R \times T$.

Assume that $(a_1, t_1) \sim (a_2, t_2)$. Then, there exist $u_1, u_2 \in R$, such that,

$$t_1 u_2 = t_2 u_1 \in T \tag{I.46}$$

$$a_1 u_2 = a_2 u_1. \tag{I.47}$$

Claim:

$$\textit{If } \exists\, a, a' \in R: \;\; t_1 a = t_2 a' \in T \tag{I.48}$$

$$\textit{then } a_1 a = a_2 a'$$

Indeed, there exists $\tilde{a} \in R$, $\tilde{t} \in T$, such that,

$$(t_1 u_2)\tilde{a} = (t_1 a)\tilde{t} \tag{I.49}$$

$$(t_2 u_1)\tilde{a} = (t_2 a')\tilde{t}, \textit{ by replacing with } (I.46) \textit{ and } (I.48) \tag{I.50}$$

$$u_2 \tilde{a} = a\tilde{t}, \textit{ by cancelling } t_1 \textit{ in } (I.49) \tag{I.51}$$

$$u_1 \tilde{a} = a'\tilde{t}, \textit{ by cancelling } t_2 \textit{ in } (I.50) \tag{I.52}$$

Now, consider $a_1 a\tilde{t}$,

$$a_1 a\tilde{t} = a_1 u_2 \tilde{a}, \textit{ by multiplying with } a_1 \textit{ in } (I.51)$$

$$a_1 u_2 \tilde{a} = a_2 u_1 \tilde{a}, \textit{ by replacing with } (I.47)$$

$$a_2 u_1 \tilde{a} = a_2 a'\tilde{t}, \textit{ by replacing with } (I.52)$$

So, $a_1 a\tilde{t} = a_2 a'\tilde{t}$, hence, $a_1 a = a_2 a'$ and the claim holds.

Let us write a/t for the class containing (a, t) and call a the **numerator** and t the **denominator** of this expression. We note that (I.44) now holds by definition, and it may be interpreted as saying that two fractions are equal if and only if when they are brought to a common denominator, their numerators agree.

It follows from (I.42) that any two expressions can be brought to a common denominator (see also the common denominator lemma for rings, lemma I.3.9, page 24). For this reason, we can define the addition of fractions by the rule

$$a/t + b/t := (a+b)/t. \tag{I.53}$$

We check that this sum is well defined, i.e., that the expression on the right depends only on a/t, b/t and not on a, b, t. For this, assume $a/t = a'/t'$ *and* $b/t = b'/t'$. Then, there exist x, $y \in R$ such that $tx = t'y$. Hence, by the claim proved above, we have $ax = a'y$ and $bx = b'y$, thus,

$$\begin{aligned} (a+b)x &= (a'+b')y \\ tx &= t'y. \end{aligned}$$

So, $(a+b)/t = (a'+b')/t'$. This justifies the definition of addition. Since two fractions can be reduced to the same denominator, we see that the addition is associative and commutative, that $0/1$ is the *zero* element, and that the additive inverse of a/t is $(-a)/t$.

Since definition (I.45) of the equivalence relation is the same as definition (I.7) (see page 9) of the equivalence relation defined in the proof of theorem I.2.5, Ore's embedding for a monoid (see page 8), we can apply theorem I.2.5 to the multiplicative monoid of R, and then, we have a well defined associative product compatible with "$\sim$", as follows (see (I.22), page 11): given $(a_1, t_1), (a_2, t_2) \in \Delta$, we can find, $u_1 \in T, u_2 \in R$, such that

$$t_1 u_2 = a_2 u_1. \tag{I.54}$$

Now, define

$$(a_1, t_1).(a_2, t_2) := (a_1 u_2, t_2 u_1). \tag{I.55}$$

Define $R_T := \Delta/\sim$ with the induced operations "+" and "." .

Note that $a/t \,.\, 1/1 = 1/1 \,.\, a/t = a/t$, so, $1/1$ is the unity; and for all $t \in T$, $1/t \,.\, t/1 = t/1 \,.\, 1/t = 1/1$, so, $t/1$ is invertible, for all $t \in T$.

On the other hand, $a/t = (a/1).(1/t) = (a/1).(t/1)^{-1}$, hence to verify the distributive law, it is sufficient to verify the equations

$$\begin{aligned}(a/1).(b/t + b'/t) &= (a/1).(b/t) + (a/1).(b'/t),\\ (b/t + b'/t).(a/1) &= (b/t).(a/1) + (b'/t).(a/1),\end{aligned}$$

which follow from the definition of "+" and ".". Thus, R_T is a ring and $R_T = RT^{-1}$. Define a mapping $\lambda\colon R \longrightarrow R_T$ given by $a \mapsto a/1$. It is routine to check that it is a T–inverting ring homomorphism.

Given a T–inverting ring homomorphism $f\colon R \longrightarrow R'$, where R' is another ring, define $\tilde{f}\colon R_T \longrightarrow R'$ by mapping $\lambda(a)$ to $f(a)$ and $\lambda(t)^{-1}$ to $f(t)^{-1}$ ($t \in T, a \in R$), which exists in R' by assumption. Any relation in R_T is a consequence of relations in R and relations expressing that $1/t$ is the inverse of $\lambda(t) = t/1$. Since all these relations still hold in R' (since f is T–inverting), $\tilde{f}$ is well defined and it is clearly a homomorphism, by construction. It is unique because its values are prescribed on $\lambda(R)$ and $\lambda(R)^{-1}$, which generate R_T since $R_T = RT^{-1}$. So, (R_T, λ) is the universal T–inverting ring on R.

Finally, *ker* λ consists of all $a/1 = 0/1$, i.e., by (I.44), all a such that $at = 0$, for some $t \in T$. ∎

An important case is that where T lies in the centre of R, in particular, if R is commutative. Then, (I.42) and (I.43) are automatic and we have:

Corollary I.3.10 *Let R be a ring and T any multiplicative submonoid of R that lies in the centre of R. Then, T is a reversible Ore set and the universal T–inverting ring R_T consists of all fractions a/t ($a \in R$), where*

$$a/t = a'/t' \longleftrightarrow a'/t' = ta'. \;\blacksquare$$

The condition of theorem I.3.8 (see page 23) simplify slightly when T consists entirely of regular elements (recall that an element of a ring is **regular** if it is not a right or left zero divisor, and also, a subset of a ring R is **regular** if its elements are regular). The (I.43) is superfluous and $\ker \lambda = 0$, so, λ is injective. We state this as

Corollary I.3.11 (Ore's embedding for a ring) *Let R be a ring and T be a multiplicative right Ore subset of regular elements. Then, the natural homomorphism $\lambda: R \longrightarrow R_T$ is injective.* ∎

The subset T of all regular elements in R is always a multiplicative submonoid of R and satisfies (I.43). When it satisfies (I.42), we can form R_T; this is called the **total (classical) quotient ring**. Generally, one understands by a **quotient ring** a ring in which every regular element is a unit.

Finally, we note the special case of integral domains which was the original case treated by Ore. Writing $R^\times = R/0$, we have

Corollary I.3.12 (Ore's embedding for integral domains) *Let R be an integral domain such that*

(I.56) $$aR \cap bR \neq 0, \text{ for all } a,\ b \in R^\times.$$

Then, $R^\times$ is a regular Ore set, $K = R_{R^\times}$ is a skew field and the natural mapping $\lambda: R \longrightarrow K$ is an embedding. Conversely, if R is an integral domain with an embedding in a skew field whose elements all have the form ab^{-1}, ($a \in R,\ b \in R^\times$), then (I.56) holds. ∎

The skew field K occurring here is an instance of a field of fractions (see definition I.3.6, page 21) of R. An integral domain satisfying (I.56) is called a **right Ore domain**; **left Ore domain** are defined similarly and an **Ore domain** is a domain which is left and right Ore.

Given a ring R and a subset $A \subset R$, by $Z_R(A)$ we mean the **centralizer** of A in R, i.e. the set of all elements of R that commute with every element of A.

It is an interesting observation made by Goldie that the Ore condition is a consequence of the Noetherian condition.

Lemma I.3.13 *Let R be an integral domain. Let $a, b \in R^\times$ such that $aR \cap bR = 0$ ($Ra \cap Rb = 0$). Then, the elements b, ab, a^2b, a^3b, ... are right (left) linearly independent over R. In particular, they are linearly independent over the centre of R or over any subring k of R, such that $k \subset Z_R(\{a^i b\}_{i \in \mathbb{N} \cup \{0\}})$.*

Proof. We give the proof for the right version, the left one being similar. Suppose not, assume $\sum a^i b c_i = 0$, for some $c_i \in R$, and let c_v be the first non-zero coefficient. We can cancel a^v and obtain the relation $bc_v + abc_{v+1} + \ldots + a^{n-v} bc_n = 0$, i.e.

$$a(bcv + 1 + \ldots + a^{n-1-v} bc_n) = -bc_v \neq 0,$$

and this contradicts the assumption $aR \cap bR = 0$. The proof for the left version is similar. ∎

Proposition I.3.14 *Any integral domain is either a right (left) Ore domain or it contains free right (left) ideals of infinite rank. In particular, any right (left) Noetherian domain is right (left) Ore.*

Proof. We shall prove the right version of this proposition, the left one being similar. Let R be an integral domain and suppose that R is not right Ore. Then, there exist $a, b \in R^\times$ such that $aR \cap bR = 0$; now, the conclusion follows from lemma I.3.13 above. ∎

It is important to observe that the field of fractions of a right Ore domain is essentially unique. Because without Ore's conditions this result need not hold, indeed, we shall see in section I.6 a family of rings with countably many non-isomorphic fields of fractions.

Let us first note that the construction is functorial. Thus, given a map between pairs $f: (R,T) \longrightarrow (R',T')$, i.e. a homomorphism $f: R \longrightarrow R'$ such that $f(T) \subset T'$, then we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\lambda} & R_T \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f_1} \\ R' & \xrightarrow[\lambda']{} & R'_{T'} \end{array}$$

and by the universal property of R_T there is a unique map $f_1 : R_T \longrightarrow R'_{T'}$ such that the resulting square commutes. In particular, if f is an isomorphism, so is f_1.

So far R, R' have been quite general; suppose now that R is a right Ore domain and K is any field of fractions of R, thus we have an embedding $f : R \hookrightarrow K$. If $T = R^\times$, we have a homomorphism $f_1 : R_T \longrightarrow K$, which we claim is injective. For, if $at^{-1} \in Ker\, f$, then $0 = f_1(at^{-1}) = f(a)f(t)^{-1}$, hence $f(a) = 0$, and so $a = 0$, because f is injective. It follows that f_1 is an embedding; the image is a field containing R and hence equal to K, because K was a field of fractions. Thus, f_1 is an isomorphism and we have

Proposition I.3.15 *The field of fractions of a right Ore domain is unique up to isomorphism.* ∎

This result is of particular interest because it ceases to hold for more general rings; we shall see examples of rings having several non-isomorphic fields of fractions (see section I.6, page 46).

If R is a ring and T a right Ore set in R, then any T-inverting homomorphism $f: R \longrightarrow S$ extends in a unique fashion to a homomorphism of R_T into R, by the universal property of R_T (see definition I.3.3, page 20). But actually, we can get an extension property, under a certain condition, for R-subrings of R_T.

Proposition I.3.16 *Let $f: R \longrightarrow S$ be an injective homomorphism. If T is a right Ore set in R, such that $f(T)$ is regular (i.e., no element of $f(T)$ is a right or left zero divisor), and R' is an R-subring of R_T such that*

$$a \in R'.b \ (a \in R,\ b \in T) \longrightarrow f(a) \in S.f(b), \tag{I.57}$$

then, f extends to a unique homomorphism $f': R' \longrightarrow S$ and f' is again injective.

Proof: Let $r \in R'$, write $r = ab^{-1}$, $a \in R$, $b \in T$ (since T is right Ore), so $a = rb$ and, hence, by (I.57), $f(a) = sf(b)$, *for some* $s \in S$. We define $f'(r) := s$ and note that if instead of a, b we had used au, bu, *where* $bu \in T$, then, $f(au) = sf(bu)$ with the same s. Indeed, assume $f(au) = s'f(bu)$, *for some* $s' \in S$; since $f(T)$ is regular and $bu \in T$, then $f(bu)$ is cancellable, so

$$\begin{aligned} f(a) &= sf(b) \\ f(a)f(u) &= sf(b)f(u) \\ f(au) &= sf(bu) \\ s'f(bu) &= sf(bu) \\ s' &= s. \end{aligned}$$

So, any expression $r = au(bu)^{-1}$ leads to the same value of $f'(r)$. Since any two expressions of r can be brought to a common denominator, they lead to the same value of $f'(r)$, so f' is well defined. The homomorphism property follows as in the proof of theorem I.3.8, page 23, and injectivity as in the proof of proposition I.2.7, page 15. ∎

I.4 Skew polynomial rings[2]

[2] Also called **twisted polynomial rings** or **differential polynomial rings**.

In commutative ring theory the polynomial ring $R[x]$ in an indeterminate x plays a basic role. The corresponding concept for general rings is the ring freely generated by an indeterminate x over R, i.e., the **tensor ring** $R_A\langle x\rangle$, where A is the prime subring of R, that is, the subring of R generated by 1 (thus $R_A\langle x\rangle$ is the R–ring generated by x with defining relations $\alpha x = x\alpha$ for all $\alpha \in A$). The elements of $R_A\langle x\rangle$ are not like the usual polynomials, but to simplify matters, we shall consider those rings whose elements can be written in the form of polynomials. Thus, for a given ring R we consider a ring P whose elements can be written uniquely in the form

$$f = a_0 + xa_1 + \ldots + x^n a_n, \text{ where } a_i \in R. \tag{I.58}$$

As usual we define the **degree** of f as the highest power of x which occurs with non–zero coefficient, so

$$d(f) := max\{i : a_i \neq 0\}, \text{ if } f \neq 0, \text{ and set } d(0) = -\infty. \tag{I.59}$$

We shall characterize the ring P under the assumption that the degree has the usual properties:

D.1 $d(f) \geq 0$ *for* $f \neq 0$, $d(0) = -\infty$,

D.2 $d(f-g) \leq max\{d(f),\ d(g)\}$,

D.3 $d(fg) = d(f) + d(g)$.

An integer–valued function d on a ring satisfying **D.1–3** is called a **degree function** (essentially this means that $-d$ is a valuation, for the definition of a valuation, see page 44). Leaving aside the trivial case $R = 0$, we see from **D.3** that P is an integral domain and moreover, for any $a \in R^\times$, ax has degree 1, so there exist a^α, a^δ such that

$$ax = xa^\alpha + a^\delta. \tag{I.60}$$

When $\delta = 0$ (I.60) is called the **Hilbert's twist**.

By the uniqueness of the form (I.58), the elements a^α, a^δ are uniquely determined by a, and $a^\alpha = 0$ iff $a = 0$. By (I.60), we have $(a+b)x = x(a+b)^\alpha + (a+b)^\delta$, $ax + bx = xa^\alpha + a^\delta + xb^\alpha + b^\delta$, hence on comparing the right-hand sides we find

$$(a+b)^\alpha = a^\alpha + b^\alpha,\ (a+b)^\delta = a^\delta + b^\delta, \tag{I.61}$$

so, α and δ are additive mappings of R into itself. Next, we have $(ab)x = x(ab)^\alpha + (ab)^\delta$, $a(bx) = a(xb^\alpha + b^\delta) = (xa^\alpha + a^\delta)b^\alpha + ab^\delta$, hence

$$(ab)^\alpha = a^\alpha b^\alpha,\ (ab)^\delta = a^\delta b^\alpha + ab^\delta. \tag{I.62}$$

Finally, $1.x = x.1 = x.1^\alpha + 1^\delta$, so

$$1^\alpha = 1,\ 1^\delta = 0. \tag{I.63}$$

The first equation in (I.61), (I.62) and (I.63) shows that α is a ring homomorphism, and by the remark following (I.60) it is injective. The remaining equations now show δ to be an α-derivation.

We next observe that the commutation rule (I.60), with the uniqueness of (I.58) is enough to determine the multiplication in P. For by the distributive law we need only know $x^m a.x^n b$ and by (I.60) the effect of moving a past a factor x is

$$x^m a x^n b = x^{m+1} a^\alpha x^{n-1} b + x^m a^\delta x^{n-1} b.$$

Now an induction on n allows us to write $x^m a x^n b$ as a polynomial in x. Thus, P is completely determined when α, δ are given. We shall call P a **skew polynomial ring** in x over R relative to the endomorphism α and α-derivation δ, and write $P = R[x; \alpha, \delta]$. Thus, we have proved the first part of

Theorem I.4.1 (Characterization of skew polynomial rings) *Let P be a ring whose elements can be expressed uniquely as polynomials in x with coefficients in an non-trivial ring R, as in (I.58), with a degree function defined by (I.59), and satisfying the commutation rule (I.60). Then, R is an integral domain, α is an injective endomorphism, δ is an α-derivation and $P = R[x; \alpha, \delta]$ is the skew polynomial ring in x over R, relative to α and δ. Conversely, given an integral domain R with an injective endomorphism α and an α-derivation δ, there exists a skew polynomial ring $R[x; \alpha, \delta]$.*

Proof. It only remains to prove the converse. Consider the set $R^{\mathbf{N}}$ of all sequences $(a_i) = (a_0, a_1, \ldots)$, $a_i \in R$, as a right R-module. Besides the right multiplication by R we have the additive group endomorphism

$$x : (a_i) \longrightarrow (a_i^{\delta} + a_{i-1}^{\alpha}), \text{ where } a_{-1} = 0. \tag{I.64}$$

Clearly, R acts faithfully on $R^{\mathbf{N}}$ by right multiplication, so we may identify R with its image in $E = End_{\mathbf{Z}}(R^{\mathbf{N}})$. Let P be the subring of E generated by R and x; we claim that P is the required skew polynomial ring. To verify (I.60), we check that the endomorphism ax and $xa^{\alpha} + a^{\delta}$ agree on each component of any sequence of $R^{\mathbf{N}}$; we have

$$(c_i)ax = (c_i a)x \tag{I.65}$$

$$= ((c_i a)^{\delta} + (c_{i-1}a)^{\alpha} \tag{I.66}$$

$$= (c_i^{\delta}a^{\alpha} + c_i a^{\delta} + c_{i-1}^{\alpha}a^{\alpha}) \tag{I.67}$$

$$(c_i)(xa^{\alpha} + a^{\delta}) = (c_i^{\delta}a^{\alpha} + c_{i-1}^{\alpha}a^{\alpha} + c_i a^{\delta}). \tag{I.68}$$

Hence, $ax = xa^{\alpha} + a^{\delta}$ in P, and (I.60) holds. It follows that every element of P can be written as a polynomial (I.58), and this expression is unique, for we

have

$$(1,0,0,\ldots)(a_0 + xa_1 + \ldots + x^n a_n) = (a_0, a_1, \ldots, a_n, 0, \ldots),$$

so distinct polynomials represent different elements of P. Finally it is clear that $d(f)$ defined as in (I.59) is a degree function, because R is an integral domain, (I.60) holds and α is injective. So, P is indeed a skew polynomial ring. ∎

It is important to observe that the construction of the skew polynomial ring is not left–right symmetric, and besides $R[x;\alpha,\delta]$ we can also introduce the **left skew polynomial ring**, in which the coefficients are written on the left. The commutation rule (I.60) then has to be replaced by

$$xa = a^\alpha x + a^\delta. \tag{I.69}$$

In general the left and right skew polynomial rings are distinct, but when α is an automorphism of R there is no need to distinguish between them as proposition I.4.3 below shows. But, first, we need the following

Lemma I.4.2 *Let K be a field, possibly skew, with an injective endomorphism α and an α–derivation δ. Let $A = K[x;\alpha,\delta]$ be a skew polynomial ring over K. Let $\alpha\colon K \longrightarrow K$ be a non–surjective endomorphism. Let $c \in K$, $c \notin K^\alpha$. Then, $Ax \cap Axc = 0$. In particular, A is not a left Ore domain.*

Proof. Suppose not, then for some $f,\ g \in A^*$,

$$fx = gxc. \tag{I.70}$$

Comparing degrees in (I.70) we see that $\deg f = \deg g = n$, say. Let $f = x^n a + \ldots$, $g = x^n b + \ldots$, then by comparing highest terms in (I.70) we find $a^\alpha = b^\alpha c$, hence $c = (b^{-1}a)^\alpha$, and this contradicts the choice of c. ∎

Proposition I.4.3 *Let K be an integral domain with an injective endomorphism α and an α–derivation δ.*

If α is an automorphism of K, then the ring $A = K[x;\alpha,\delta]$ is a left skew polynomial ring.

If, in addition, K is a skew field, then the converse holds, i.e. if $A = K[x;\alpha,\delta]$ is a left skew polynomial ring, where K is a skew field, then α is an automorphism of K.

Proof. If α is an automorphism of K, with inverse β say, then on replacing a by a^β we can write (I.60) (see page 32) as $a^\beta x = xa + a^{\beta\delta}$, i.e.

$$xa = a^\beta x - a^{\beta\delta},$$

which is of the form (I.69). So, the ring A is a left skew polynomial ring.

Now, suppose that K is a field and assume that α is not an automorphism, then it is not surjective (since K is a field and our homomorphisms preserve 1) and so there exists $c \in K$, $c \notin K^\alpha$. Then, by lemma I.4.2 above, $Ax \cap Axc = 0$. So, A is not a left Ore domain. Hence, by the left version of proposition I.3.14 (see page 29), A is not left Noetherian, so, it can not be left principal. ∎

Corollary I.4.4 *Let K be a skew field with an injective endomorphism α and an α-derivation δ. The ring $A = K[x;\alpha,\delta]$ is a left skew polynomial ring if and only if α is an automorphism of K.* ∎

The Hilbert basis theorem extends to skew polynomial rings relative to an automorphism. The proof is essentially the same as in the commutative case.

Theorem I.4.5 (Hilbert basis theorem for skew polynomial rings) *Let R be a right Noetherian domain, α an automorphism and δ an α-derivation of R. Then, the skew polynomial ring $A = R[x;\alpha,\delta]$ is again a right Noetherian domain.*

Proof. By proposition I.4.3, we can consider A as a left skew polynomial ring, i.e. with coefficients on the left. If A is not right Noetherian, let $\mathfrak{a}$ be a right

ideal which is not finitely generated. Let $f_1 \in \mathfrak{a}$ be a non–zero polynomial of least degree; given $f_1, \ldots, f_k \in \mathfrak{a}$, we take $f_{k+1} \in \mathfrak{a} \backslash \sum_{i=1}^{k} f_i A$ of least degree. Since $\mathfrak{a}$ is not finitely generated, we thus obtain an infinite sequence $f_1, f_2, \ldots$; let f_i have degree n_i and leading coefficient a_i, then $n_1 \leq n_2 \leq \ldots$. We claim that $a_1 R \subset a_1 R + a_2 R \subset \ldots$ is an infinite ascending chain, which will contradict the fact that R is right Noetherian. For an equation $a_{k+1} = \sum_{i=1}^{k} a_i b_i$ $(b_i \in R)$ would mean that

$$g := f_{k+1} - \sum_i f_i b_i^{\alpha^{-n_i}} x^{n_{k+1}-n_i} \in \mathfrak{a} \backslash \sum_{i=1}^{k} f_i A,$$

but g has lower degree than f_{k+1}, which is a contradiction. ∎

In the construction of skew polynomial rings it was necessary to start from an integral domain because we insisted on a degree function; this is not essential, but it is the case mostly used in applications. Frequently the coefficient ri will even be a field, possibly skew. In that case the skew polynomial ring is a principal right ideal domain; this follows, as in the commutative case, using the division algorithm (see proposition I.4.7 below).

Proposition I.4.6 (Division algorithm for skew polynomial rings) *Let R be an integral domain with an injective ring endomorphism α and α–derivation δ. Let $A = R[x; \alpha, \delta]$. Assume $f, g \in A$, where the leading coefficient of g is a unit in R. Then, there exist unique $q, r \in A$ such that*

$$f = gq + r, \text{ where } \deg r < \deg g.$$

Proof. First, we show existence. Let m be the degree of f and n the degree of g. If $m < n$ then we take $q = 0$ and $r = f$.

If $m \geq n$, then we use induction on m. If $m = 0$, then $n = 0$, so we can take $q = g^{-1} f$, and $r = 0$. If $m > 1$, let $x^m a$, $x^n b$ be the respective leading terms of f, g. Note that $x^m a = x^n b(b^{-1} x^{m-n} a)$. Let $h = f - g b^{-1} x^{m-n} a$. Since

deg $h < m$, we can write, by induction, $h = gq' + r$, for some q', $r \in A$, with $r = 0$ or deg $r <$ deg g. So, $f = h + gb^{-1}x^{m-n}a = (gq' + r) + gb^{-1}x^{m-n}a = g(q' + b^{-1}x^{m-n}a) + r$.

We now show uniqueness. If $gq + r = g\tilde{q} + \tilde{r}$, where

$$\text{(I.71)} \qquad \begin{cases} \deg r < \deg g, \\ \deg \tilde{r} < \deg g, \end{cases}$$

then

$$\text{(I.72)} \qquad r - \tilde{r} = g(\tilde{q} - q).$$

By **D.2** (see page 32), we have

$$\deg (r - \tilde{r}) \leq \max \{\deg r, \deg \tilde{r}\}$$

and by (I.71)

$$\max \{\deg r, \deg \tilde{r}\} < \deg g.$$

So,

$$(*) \qquad \deg (r - \tilde{r}) < \deg g.$$

From (I.72) and the degree formula (I.59) (see page 32) we have deg $(r - \tilde{r}) =$ deg $(q - \tilde{q}) +$ deg g. If $r - \tilde{r} \neq 0$, then deg $(r - \tilde{r}) \geq$ deg g, contradicting $(*)$. So, $r - \tilde{r} = 0$.

Since the principal coefficient of g is a unit in R, then, in particular $g \neq 0$, and since A is a domain (by theorem I.4.1, see page 33), it follows from (I.72) that $\tilde{q} - q = 0$. ∎

Proposition I.4.7 *Any skew polynomial ring $K[x;\alpha,\delta]$ over a field K is a principal right ideal domain.*

Proof. Let $\mathfrak{a}$ be a non–zero right ideal of K. Let f be a monic polynomial of least degree in $\mathfrak{a}$. Then, every non–zero $g \in \mathfrak{a}$ can be written as $g = fq + r$, where $\deg r < \deg f$, by proposition I.4.6. Since $r = g - fq \in \mathfrak{a}$, it follows that $r = 0$ and so $g \in fR$. Then, $\mathfrak{a} = fR$. So, K is a principal right ideal domain. ∎

In particular, for a skew field K, the skew polynomial ring $K[x;\alpha,\delta]$ is right Noetherian (because it is right principal), and hence it is right Ore, by proposition I.3.14 (see page 29), so we can form its skew field of fractions. This is denoted $K(x;\alpha,\delta)$; its elements are fractions fg^{-1}, where f, g are polynomials (I.58) with coefficients in K.

Let R, A, B be any rings, $\alpha\colon R \longrightarrow A$, $\beta\colon R \longrightarrow B$ two homomorphisms and M an (A, B)–bimodule. Then an **(α,β)–derivation** from R to M is a map $\delta\colon R \longrightarrow M$ which is additive and satisfies

$$\delta(xy) = \alpha(x)\delta(y) + \delta(x)\beta(y). \tag{I.73}$$

In particular, if $A = R$ and $\alpha = 1$, we speak of a **(right) β–derivation**. Putting $x = y = 1$ in (I.73) and observing that $\alpha(1) = \beta(1) = 1$, we see that any (α, β)–derivation satisfies

$$\delta(1) = 0. \tag{I.74}$$

It is easily verified that *ker* δ is a subring of R called the **ring of constants** (with respect to δ). Moreover, any element of *ker* δ which is invertible in R is also invertible in *ker* δ, as follows by the formula (itself easily checked):

$$\delta(x^{-1}) = -\alpha(x^{-1}).\delta(x).\beta(x^{-1}). \tag{I.75}$$

With any (A, B)–bimodule M we can associate the ring $\begin{pmatrix} A & M \\ 0 & B \end{pmatrix}$ consisting of all matrices

$$\begin{pmatrix} a & m \\ 0 & b \end{pmatrix} \quad (a \in A, b \in B, m \in M),$$

with the usual matrix addition and multiplication.

Given maps $\alpha: R \longrightarrow A$, $\beta: R \longrightarrow B$, $\delta: R \longrightarrow M$, we can define a map from R to $\begin{pmatrix} A & M \\ 0 & B \end{pmatrix}$ by the rule

$$x \mapsto \begin{pmatrix} \alpha(x) & \delta(x) \\ 0 & \beta(x) \end{pmatrix}, \tag{I.76}$$

and it is easily checked that this is a ring homomorphism iff α, β are homomorphisms and δ is an (α, β)–derivation. This alternative method of defining derivations is often useful, for instance, in the following

Theorem I.4.8 *Let R, A, B be rings, T a multiplicative subset of $R^\times$ and M an (A, B)–bimodule. Then, any T–inverting homomorphism $\alpha: R \longrightarrow A$ extends to a unique homomorphism $\alpha': R_T \longrightarrow A$, and given T–inverting homomorphisms $\alpha: R \longrightarrow A$, $\beta: R \longrightarrow B$, any (α, β)–derivation $\delta: R \longrightarrow M$ extends to an (α', β')–derivation of R_T into M.*

Proof. The existence and uniqueness of α' follows because R_T is universal T–inverting. Now, δ defines a homomorphism (I.76) from R to $\begin{pmatrix} A & M \\ 0 & B \end{pmatrix}$, which is T–inverting and therefore extends to a homomorphism of R_T:

$$x \mapsto \begin{pmatrix} \alpha'(x) & \delta'(x) \\ 0 & \beta'(x) \end{pmatrix}.$$

It follows that δ' is an (α', β')–derivation. ∎

Proposition I.4.9 *Any skew polynomial ring over a right Ore domain is again right Ore.*

Proof. Let R be a right Ore domain and K its field of fractions. If α is an injective endomorphism of R and δ an α–derivation, they can be extended to K, by theorem I.4.8, and we have the inclusions

$$R[x;\alpha,\delta] \subset K[x;\alpha,\delta] \subset K(x;\alpha,\delta).$$

Any element $u \in K(x;\alpha,\delta)$ has the form fg^{-1}, where $f,\ g \in K[x;\alpha,\delta]$. By lemma I.3.9 (see page 24), we can bring the finite set of coefficients of $f,\ g$ to a common denominator, say $f = f_1c^{-1},\ g = g_1c^{-1}$, where $f_1,\ g_1 \in R[x;\alpha,\delta]$, *and* $c \in R^\times$. Now $u = f_1c^{-1}(g_1c^{-1})^{-1} = f_1g_1^{-1}$, so every element of $K(x;\alpha,\delta)$ can be written as a right fraction of elements of $R[x;\alpha,\delta]$, and hence the latter is right Ore, by corollary I.3.12 (see page 28). ∎

I.5 Examples of Skew polynomial rings

We shall see some examples of skew polynomial rings. When the derivation is 0, we write $R[x;\alpha]$ in place of $R[x;\alpha,0]$.

Example 1: $\alpha = 1,\ \delta = 0$. We obtain the ordinary polynomial ring $R[x]$ in a central indeterminate (although R does not need to be commutative).

Example 2: The **complex–skew polynomial ring** $\mathbb{C}[x;-]$ is the ring of polynomials with complex coefficients and commutation rule

$$ax = x\overline{a},\ \textit{where } \overline{a} \textit{ is the complex conjugate of } a.$$

The centre of this ring is the ring $\mathbb{R}[x^2]$ of all real polynomials in x^2, and $\mathbb{C}[x;-]/(x^2+1)$ is the division algebra of real quaternions (cf. [Lam91], page 25).

More generally, let k be a field of characteristic not 2 with a quadratic extension $K = k(\sqrt{b})$; this has an automorphism α given by $(x + y\sqrt{b})^\alpha = x - y\sqrt{b}$. For any $a \in k^\times$, $K[x;\alpha]/(x^2 - a)$ is the quaternion algebra $(a, b; k)$.

Example 3: Let K be any commutative ring and denote by $A_1[K]$ the K–algebra generated by u, v over K with the relation

$$uv - vu = 1 \tag{I.77}$$

This ring is called the **Weyl algebra** on u, v *over* K. It may also be defined (cf. [Lam91], page 7) as the skew polynomial ring $R[v; 1, ']$, where $R = K[u]$ and $'$ denotes differentiation with respect to u. We observe that when K is a Noetherian domain, then so is $A_1[K]$ because $A_1[K]$ is a twisted polynomial ring over $K[y]$ (cf. [Lam91], page 8).

From (I.77), we obtain by induction on n,

$$u^n v - v u^n = n u^{n-1},$$

hence $u^m v^n . v - v . u^m v^n = m u^{m-1} v^n = \partial(u^m v^n)/\partial u$. A similar formula holds for commutation by u and by linearity it follows that for any $f \in A_1[K]$,

$$fv - vf = \frac{\partial f}{\partial u},\ uf - fu = \frac{\partial f}{\partial v}. \tag{I.78}$$

From these formulae it is easy to show that for a field k of characteristic 0, $A_1[k]$ is a simple ring. For, if $\mathfrak{a}$ is a non–zero ideal in $A_1[k]$, pick an element $f(u, v) \neq 0$ in $\mathfrak{a}$ of least possible degree in u. Then $\partial f/\partial u = fv - vf \in \mathfrak{a}$, but this has lower u–degree and so must be 0. Hence $f = f(v)$ is a polynomial in v alone. If its v–degree is taken minimal, then $df/dv = uf - fu = 0$ and so $f = c \in k$. Thus $\mathfrak{a}$ contains a non–zero element of k and so must be the whole ring, i.e. $A_1[k]$ is simple, as claimed.

We observe that $A_1[k]$ is an example of a simple Noetherian domain, not a

field. For a field k of finite characteristic p, $A_1[k]$ is no longer simple, since it has centre $k[u^p, v^p]$.

Example 4: The **translation ring** $k<x, y|xy = y(x+1)>$ may be described as $R = A[y; \sigma]$, where A is the polynomial ring $k[x]$ with the **shift automorphism** $\sigma : x \longrightarrow x + 1$.

Example 5:

Let k be a field of prime characteristic p and $F : a \longrightarrow a^p$ the **Frobenius endomorphism**. Then $k[x; F]$ is a skew polynomial ring whose field of fractions $k(x; F)$ has an inner automorphism inducing F, namely conjugation by x.

More generally, if k is any field, even skew, with an endomorphism α, then $k(x; \alpha)$ is an extension with an inner automorphism inducing α on k, because (I.60) now reads $ax = xa^\alpha$. Similarly, if δ is an α–derivation, then $k[x; \alpha, \delta]$ is a ring with an inner α–derivation inducing δ, as we see by writting (I.60) in the form

$$a^\delta = ax - xa^\alpha.$$

Example 6:

Let K be a commutative field with automorphism α of order n, and consider the skew field of fractions $E = K(x; \alpha)$. If k is the fixed field of α, the $F = k(x^n)$ is contained in the centre of E, as may be checked (cf. [Lam91], page 250). Moreover, $K(x^n)$ is a commutative subfield, a Galois extension of F of degree n, and provided that K contains a primitive n–th root of 1, the structure of E is given by the equations

$$ax^i = x^i a^{\alpha^i}, \text{ for all } a \in K, i = 0, 1, \ldots, n-1.$$

It follows that $k(x^n)$ is the precise centre of E and E is of dimension n^2 over its centre, in fact a crossed product[3]. (Let R be a ring and G be a group.

[3] For an introduction to crossed products, see, for instance, [MR87], 1.5.1

Let S be a ring containing R and containing a set of units $\overline{G} := \{\overline{g} : \ g \in G\}$ isomorphic as a set to G such that: i) S is free as right R–module with $\overline{G}$ as a basis and $\overline{1}_G = 1_S$; and ii) for all $g_1, g_2 \in G$, $\overline{g}_1 R = R\overline{g}_1$ and $\overline{g}_1\overline{g}_2 R = \overline{g_1 g_2}R$. Then S is called a **crossed product** of R by G, written $R * G$).

Example 7:

Let R be an integral domain with an automorphism α. In the skew polynomial ring $R[x;\alpha]$ the powers of x form an Ore set, and the ring of fractions consists of all polynomials $\sum_{-r}^{s} x^i a_i$, involving negative as well as positive powers of x. Such an expression is called a **skew Laurent polynomial** and the resulting ring may be written $R[x, x^{-1}; \alpha]$.

For each polynomial f of the form (I.58) we can also define its **order** $o(f)$ as the lowest power of x occurring with a non–zero coefficient:

$$o(f) = min\{i|\ a_i \neq 0\}, \quad o(0) = \infty.$$

This function has the properties of a **valuation** on P:

O.1 $o(f) \geq 0$ *for* $f \in P$, $o(0) = \infty$,

O.2 $o(f - g) \geq min\{o(f),\ o(g)\}$,

O.3 $o(fg) = o(f) + o(g)$.

Taking first the case $\delta = 0$, we can form the ring $R[[x;\alpha]]$ of **formal power series** over R as the set of all infinite series

$$f = a_0 + xa_1 + x^2 a_2 + \dots, \tag{I.79}$$

with component–wise addition and with multiplication based on the commutation rule $ax = xa^{\alpha}$. There is of course no question of convergence here; we regard (I.79) as a series in a purely formal sense. We can describe f equally well

as an infinite sequence $(a_i) = (a_0, a_1, \ldots)$, with addition $(a_i) + (b_i) = (a_i + b_i)$ and with multiplication

$$(a_i).(b_j) = (c_k), \text{ where} c_k = \sum a_{k-j}^{\alpha^j} b_j. \tag{I.80}$$

Alternatively, we can regard $R[[x;\alpha]]$ as the completion of the skew polynomial ring $R[x;\alpha]$ with respect to the powers of the ideal generated by x; these powers define a topology called the **x–adic topology**.

Let R be a ring and α an automorphism of R. The powers of x form an Ore set in $R[[x;\alpha]]$ and by taking fractions we obtain the ring $R((x;\alpha))$ of all **formal Laurent series** or **skew (or twisted) Laurent series**

$$\sum_{-r}^{\infty} x^i a_i = x^{-r}a_{-r} + \ldots + x^{-1}a_{-1} + a_0 + xa_1 + x^2a_2 + \ldots . \tag{I.81}$$

This is again a ring, with the same multiplication (I.80); here the restriction to finitely many negative powers is necessary to ensure that the multiplication rule (I.80) makes sense. This is also the reason for taking α to be an automorphism, since now j may take negative values in (I.80).

Let us now consider a skew polynomial ring $R[x;\alpha,\delta]$, where δ may be non–zero, but α is still an automorphism, and ask whether a power series ring can be formed. If we attempt to define the multiplication of power series by means of the commutation formula (I.60), we shall find that (apart from a more complicated form for the coefficients of the product), the product cf, where $c \in R$, can not always be expressed as a power series, because there will in general be contributions to the coefficient of a given power x^r from each term $cx^n a_n$, $(n \geq r)$ and so we may have infinitely many such terms to consider. In terms of the x–adic topology we can express this by saying that left multiplication by $c \in R$ is not continuous; this follows from (I.60), because when $a^\delta \neq 0$, we have $o(ax) < o(x)$.

One way to overcome this difficulty is to introduce $y = x^{-1}$ and rewrite (I.60)

in terms of y. We find

$$\begin{aligned} ya &= a^{\alpha}y + ya^{\delta}y \\ &= a^{\alpha}y + a^{\delta\alpha}y^2 + ya^{\delta^2}y^2 = \dots, \end{aligned}$$

hence by induction we obtain

$$ya = a^{\alpha}y + a^{\delta\alpha}y^2 + a^{\delta\alpha^2}y^3 + \dots. \tag{I.82}$$

With the help of this commutation formula we can multiply power series in y and even Laurent series. We observe that in passing from x to $y = x^{-1}$ we have also had to change the side on which the coefficients are put; of course this is immaterial as long as α is an automorphism. To be precise, from any skew polynomial ring $R[x; \alpha, \delta]$ we can form a skew power series ring in x^{-1}, with coefficients on the left; in order to define Laurent series in x^{-1} we need to assume that α is an automorphism.

I.6 Examples of rings with countably many non–isomorphic fields of fractions

Proposition I.6.1 *Let R be an integral domain. Let $x,\ y \in R$ be such that $xR \cap yR = 0$ or $Rx \cap Ry = 0$. Let k be a subring of R such that $k \subset Z_R(x)$ and $k \subset Z_R(y)$. Then, the algebra generated by x and y over k is free.*

Proof. Assume that $xR \cap yR = 0$ (if $Rx \cap Ry = 0$ the proof is similar and will be omitted). Suppose that the algebra generated by x and y over k is not free, so assume that there exists a non–trivial relation between x and y. Without loss of generality, we can assume that such a non–trivial relation looks like

$$\alpha + xa + yb = 0, \text{ where } a,\ b \in R \text{ and } \alpha \in k; \tag{I.83}$$

indeed, because R is a domain, such a relation, being non–trivial, can not consist of just one monomial either in x or in y with a coefficient in k equated to zero. After some cancellation, if necessary, we may assume that the two monomials in the non–trivial relation do not begin both either with x or with y. Passing the coefficients in k to the right of x and y, we get (I.83). Since we are assuming that (I.83) is non–trivial, we may assume that a or b are not zero. Say $b \neq 0$, then on multiplying (I.83) on the right by x we have $\alpha x + xax + ybx = 0$, i.e., $ybx = x(-\alpha - ax) \in xR \cap yR$ and $ybx \neq 0$, contradiction, which shows that x and y are free over k. ∎

Corollary I.6.2 *Let R be an integral domain. Let $x,\ y \in R$ be such that $xR \cap yR = 0$ or $Rx \cap Ry = 0$. Let k be a subring of R such that $k \subset Z_R(x)$ and $k \subset Z_R(y)$. Then, the k–algebra generated by $\{x^i y\}_{i \in \mathbb{N}}$ is a free k–module of countable rank.*

Proof. Assume that $xR \cap yR = 0$ (if $Rx \cap Ry = 0$ the proof is similar and will be omitted). By proposition I.6.1 above, x and y are free over k. By lemma I.3.13 (see page 29), $\{x^i y\}_{i \in \mathbb{N}}$ generates a free k–module. ∎

Corollary I.6.3 *Let R be an integral domain with centre Z. Then, R is either a left and right Ore domain or it contains a free Z–module of countable rank.*

Proof. Assume that R is not right Ore (if R is not left Ore the proof is similar and will be omitted). Hence, there exist $x,\ y \in R^*$ such that $xR \cap yR = 0$. By proposition I.6.1 above, we know that the Z–algebra generated by x and y is free. By the above corollary I.6.2, R contains a free Z–module of countable rank. ∎

Let k be a skew field. Consider the usual polynomial ring $k[t]$ where t **is a central indeterminate** (see example 1, page 41). Since k is a skew field, it is right Noetherian, and hence, $k[t]$ is right Noetherian by theorem I.4.5 (see

page 36), so by proposition I.3.14 (see page 29) it is right Ore. Then, we can consider its field of fractions, which we denote by $k(t)$. Let $n \in \mathbb{N}, n > 1$. Let $\alpha_n : k(t) \longrightarrow k(t)$ be a non–surjective endomorphism of $k(t)$ defined by $t \mapsto t^n$, in particular, note that t is not in the image of α_n and that α_n fixes any element of k.

Let $R_n := k(t)[x; \alpha_n]$. By theorem I.4.1 (see page 33) the skew polynomial ring R_n is an integral domain. Since t does not belong to the image of α_n, then by lemma I.4.2 (see page 35) $R_n x \cap R_n xt = 0$. Note that $k \subset Z_{R_n}(t)$ because t is a central indeterminate over k and that $k \subset Z_{R_n}(x)$ because α_n fixes any element of k and for all $a \in R_n$, $ax = xa^{\alpha_n}$, (by definition of skew polynomial ring, see (I.60), page 32; recall that the α_n–derivation is zero in this application), then by proposition I.6.1, the k–subalgebra of R_n generated by $\{x, xt\}$ is a free k–algebra. Also, we note that by corollary I.6.2, the k–subalgebra of R_n generated by $\{x^i xt\}_{i \in \mathbf{N}}$ is a free k-module of countable rank. Since k(t) is a skew field, by proposition I.4.9 (see page 41) R_n is right Ore, so by corollary I.3.12 (see page 28), it can be embedded in a field of fractions F_n, say. This provides, for each $n \in \mathbb{N}$, $n > 1$, an embedding of the free k–algebra with free generators $\{x, xt\}$, which we shall denote by $k< \{x, xt\} >$.

We now show that all these fields of fractions F_n, $n \in \mathbb{N}$, $n > 1$, are different. (for the concept of field of fractions see definition I.3.6, page 21). By "different" we mean non–isomorphic as $k< \{x, xt\} >$–rings (cf. definition I.3.5 of R-ring and the definition of the category of R-rings on page 21), i.e., a ring–isomorphism between F_n and F_m, $m \neq n$, that fixes point–wise $k< \{x, xt\} >$ can not exist. (Actually, the fields of fractions F_n, $n \in \mathbb{N}$, $n > 1$, are not isomorphic as $k< \{x, xt\} >$–fields, but to see this we need to introduce the category of epic $k< \{x, xt\} >$–fields and specializations which will be done in chapter III). Indeed, first note that in F_n, $n \in \mathbb{N}$,

$$t = txx^{-1} = xt^n x^{-1}.$$

Now, assume that $\phi: F_n \longrightarrow F_m$, $n < m$, is a $k<\{x, xt\}>$-ring isomorphism. Since t and x are fixed by ϕ then

$$xt^m x^{-1} = t = \phi(t) = \phi(xt^n x^{-1}) = \phi(x)\phi(t)^n \phi(x)^{-1} = xt^n x^{-1},$$

so $xt^m x^{-1} = xt^n x^{-1}$ in F_m, hence

$$t^s = 1,$$

where $s = m - n$. This contradicts the fact that t is an indeterminate over k. ∎

So, this provides examples of rings with countably many non-isomorphic fields of fractions.

CHAPTER II

The Malcev–Neumann and Cohn embeddings

The investigation of geometries, principally by Hilbert [Hil30], with certain incidence and order properties, but lacking others (satisfying "Desargues" but not "Papus") led to the study of totally (fully) ordered division rings. The first example of a centrally infinite division ring was Hilbert's Twisted Laurent series (see page 45, and also proposition II.2.10 in page 74). The problem of constructing more general types of ordered division rings was begun by Moufang [Mou37], who embedded the group algebra of the free metabelian group of two generators into a division ring and showed that this division ring can be ordered.

Malcev [Mal48]–Neumann [Neu49a]'s construction of formal power series division rings (formal Laurent series division rings as a particular case when the group is $(\mathbb{Z}, +)$) is also related to Hilbert's example (loc. cit.), with additional motivation coming from the earlier work of Hahn [Hah07] on the embedding of ordered abelian groups into groups of Laurent series. The Malcev–Neumann embedding was put in a general algebraic setting by Higman [Hig52] and years later, Cohn [Coh65] simplified Higman's proof.

The main idea of forming Malcev–Neumann formal power series is that one can combine Hilbert's Twisted Laurent series with the usual group ring construction, even with twisted group rings to get a much bigger class of division rings. In Hilbert's example, the non–commutativity of the product arises from the twist. In the Malcev–Neumann construction, the non–commutativity of the product arises from the use of possibly non–commutative (ordered) groups and from the action of the group over the ring. In the case when only commutative (ordered) groups are used and the Hilbert twist is taken to be trivial, the idea of the construction goes back to Hahn (loc. cit.).

As an application of the Malcev–Neumann embedding we shall embed the free k–algebra over a set X into a division ring, where k is a skew field. Comparing this embedding to the Moufang embedding (loc. cit.) we get another example of a ring with non–isomorphic fields of fractions. As a second application, we shall exhibit an example of a non–Ore ring which can still be embedded in a skew field, showing that the Ore conditions are not necessary to embed a ring in a skew field.

It has been shown by Tamari [Tam53] that the universal enveloping algebra of every *finite dimensional* Lie algebra has the right common multiple condition, hence it is embeddable in a skew field. Cohn [Coh61] proved that the universal enveloping algebra of any Lie algebra can be embedded in a skew field.

We shall give all the background material (section II.4) to prove two theorems, due to Cohn [Coh61], an embedding theorem for a certain class of inverse limit semigroups (theorem II.5.1, page 88) and an embedding theorem for valuated rings satisfying some extra condition (theorem II.6.1, page 92).

Following Cohn, we shall reformulate theorem II.6.1 in a suitable way for the application we shall give in the last section of this chapter: the proof that every Birkhoff–Witt algebra is embeddable in a skew field. We shall use this to show that the universal enveloping algebra of *any* Lie algebra (not necessarily finite dimensional) is embeddable in a skew field; and also to give another proof of the

fact that the free algebra $k\langle X\rangle$ (k a commutative field, X a set) is embeddable in a skew field.

Last year, Lichtman [Lic94] simplifies Cohn's proof and gave new methods of embedding.

II.1 Ordered groups

Certain axiomatic questions in geometry led to the study of ordered division rings (cf. introduction to chapter II) and these in turn to the study of ordered division groups: every ordered group can be embedded in (the multiplicative group of) an ordered division ring (cf. [Neu49a, Neu49b]).

It will be convenient to collect at the beginning of this section the fundamental concepts and terminology we shall need about ordered sets and (left, right) ordered groups. Then, we shall give necessary and sufficient conditions due to Levi, F. W. [Lev42] and generalized by Neumann, B. H. [Neu49b] for a group to be ordered. The general criterion is an unwieldy tool, but it can be specialized to see that every torsion–free abelian group can be ordered (Levi, loc. cit.), and even that every free group can be ordered [Bir48], see also [Fuc63].

If a binary relation $\leq$ is defined on a set A with the properties

$$\text{for all } a,\ b,\ c \in A \begin{cases} \textbf{P1.}\ \text{(reflexivity)}\ a \leq a \\ \textbf{P2.}\ \text{(antisymmetry)}\ a \leq b,\ b \leq a \text{ only if } a = b \\ \textbf{P3.}\ \text{(transitivity)}\ a \leq b,\ b \leq c \text{ only if } a \leq c \end{cases}$$

then $(A, \leq)$ is called a **partially ordered set** (abbreviated: **p. o. set** or **poset**) and $\leq$ is called a **partial order** on A. The **dual** of $(A, \leq)$ is the partial order set $(A, \geq)$ where $a \geq b$ iff $b \leq a$. In this context, by the **dual assertion** we shall mean that the signs $\leq$ and $\geq$ are to be interchanged throughout. As usual, one may write $b \geq a$ for $a \leq b$, and $a < b$ (or $b > a$) to mean that $a \leq b$ and $a \neq b$. If

neither $a \leq b$ nor $b \leq a$, then a and b are called **incomparable**, and we write: $a||b$. It may happen that a relation $\leq$ satisfies only **P1.** and **P3.**; in this case we say $\leq$ is a **preorder** or a **quasiorder**. A partial order on A induces in the natural way a partial order on any subset B of A; namely, for $a,\ b \in B$ define $a \leq b$ in $(B, \leq)$ iff $a \leq b$ in $(A, \leq)$ in the original partially ordered set $(A, \leq)$. This **induced partial order** of B will be denoted by the same symbol $\leq$.

Let $(A, \leq)$, $(A', \leq)$ (the use of the same symbol $\leq$ will cause no confusion) be two p. o. sets. A mapping $a \mapsto a'$ from A into A' is called **isotone** or an **order–homomorphism** if it is **order preserving** in the sense that $a \leq b$ only if $a' \leq b'$. A mapping as above which is a bijection and isotone in both directions is said to be an **order–isomorphism** of $(A, \leq)$ onto $(A', \leq)$ and then A and A' are called **order–isomorphic**. If a bijective mapping between $(A, \leq)$ and $(A', \leq)$ **reverses order** (i.e. $a \leq b$ iff $a' \geq b'$), then it is a **dual order isomorphism**. As usual, if it is clear from the context that we mean an order–homomorphism the word "order" will be omitted. Assume that two partial orders $\leq_1$ and $\leq_2$ are defined on the same set A. Then, $\leq_2$ is an **order extension** of $\leq_1$ if for all $a,\ b \in A$, $a \leq_1 b$ only if $a \leq_2 b$. $(A, \leq)$ has the **trivial order** if for all $a,\ b \in A$, $a \leq b$ only if $a = b$. The order relation $\leq$ is called a **full (linear, total) order** or simply an **order** on A and $(A, \leq)$ a **fully ordered set** (etc.) (**f. o. set** (etc.)) or a **loset** or a **chain**, if in addition to **P1.–P3.** also

P4. for all $a,\ b \in A$, either $a < b$ or $a = b$ or $a > b$

holds. The subsets of a f. o. set are again f. o. sets under the induced partial order. A f. o. set $(W, \leq)$ is said to be **well–ordered** if every non–void subset V of W contains a **smallest element**, i.e. an element $u \in V$ such that $u \leq v$ for every $v \in V$.

An **ordered group (o. group)** is a triple $(G, ., \leq)$ such that

G1. $(G, .)$ is a group

G2. $(G, \leq)$ is an ordered set

G3. for all $a,\ b,\ c \in G$, $a \leq b$ only if $ca \leq cb$ and $ac \leq bc$.

A triple $(G, ., \leq)$ is said to be a **left ordered (l. o. group)** if, in addition to **G1.–G2.** also

GL. for all $a,\ b,\ c \in G,\ a \leq b$ only if $ca \leq cb$

holds. Similarly, we define a **right ordered (r. o. group)** if, in addition to **G1.–G2.** also

GR. for all $a,\ b,\ c \in G,\ a \leq b$ only if $ac \leq bc$

holds. Given a (left) ordered group $(G, ., \leq)$, as usual, we shall make the following abuse of language: we shall say that **a (left) order on G is given**.

In a o. group G an element a is called **positive (integral)** if $a > 1$, and **negative** if $a < 1$. If the group operation is written additively and 0 denotes the neutral element, then positivity has the usual meaning $a > 0$. The set $P = G^+$ of positive elements of G is said to be the **positive cone** (or the **integral part**) of G. This concept is a natural tool for studying orders in a group. Unfortunately, a complete survey of it is beyond the scope of this thesis. So, we shall limit ourselves to the essential properties of this concept. The same comment goes for (left) ordered groups.

Note that an order $<$ in an ordered group $(G, ., <)$ is already uniquely determined by the corresponding positive cone P, for

Proposition II.1.1 *A subset P of a group G is the positive cone of some order of G iff it satisfies the following three conditions:*

PC1. $G = P \coprod P^{-1} \coprod \{1\}$, *where* $\coprod$ *denotes the coproduct in the category of sets, i.e. "disjoint union",*

PC2. $PP \subset P$,

PC3. $gPg^{-1} \subset P$ *for all* $g \in G$.

Proof. Assume that G is an o. group. Let $x,\ y \in P$, and let $z \in G$. Then, $1 < x, 1 < y$ only if, by **G3.**, $x < xy$ and by transitivity of $<$, we get $1 < xy$ and, similarly, we have $1 = z^{-1}1z < z^{-1}xz$. Thus xy and $z^{-1}xz$ are both contained in P. So, **PC2.** and **PC3.** hold. Now, if $g \in G$ and $g < 1$, then, on multiplying by g^{-1} and by **G3.** again, we get $1 = g^{-1}g < g^{-1}$, so $g^{-1} > 1$ and **PC1.** also holds.

Conversely, suppose $P \subset G$ satisfies **PC1.**–**PC3.**, and define $x < y$ to mean $yx^{-1} \in P$. Now, if $x < y$ and $y < z$, then $zy^{-1},\ yx^{-1} \in P$ so that **PC2** yields $zx^{-1} = (zy^{-1})(yx^{-1}) \in P$ and $x < z$, so $<$ is transitive, and, readily $\leq$ is an order relation. Moreover, if $x,\ y \in G$, then by **PC1.**, precisely one of the three possibilities $yx^{-1} \in P$, $yx^{-1} = 1$ or $xy^{-1} = (yx^{-1})^{-1} \in P$. So, we either have $x < y$, or $y < x$ or $x = y$, and then $<$ is a linear order in G.

Suppose that $x < y$ and $z \in G$. Then, $yx^{-1} \in P$, so $(yz)(xz)^{-1} = yx^{-1} \in P$ and by **PC3.** we have$(zy)(zx)^{-1} = z(yx^{-1})z^{-1} \in P$. Hence, $xz < yz$ and $zx < zy$; thus G is an o. group. Finally, because $y1^{-1} = y \in P$ iff $1 < y$, P is the positive cone for G in this ordering. ∎

Observe that **PC1.–2.** says that P is a **normal subsemigroup** of G.

Note that any (right) ordered group (G, . , $\leq$) is always torsion–free. For, if $g > 1$, then $1 < g < g^2 < \ldots$ and if $g < 1$, then $1 > g > g^2 > \ldots$, so g^n is never equal to 1. However, there exist non–abelian torsion–free groups which can not be ordered. Before giving an example, first note that any group extension of a torsion–free group by a torsion–free group must be torsion–free, in other words, if we have a short exact sequence of groups $0 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 0$ where K and Q are torsion–free then G must also be torsion–free. Indeed, assume that a group G has a quotient $Q \cong G/K$, where Q and K are torsion–free, then if $g \in G$ and $g^n = 1,\ n \in \mathbb{N}$, then $(gK)^n = g^nK = K$ and since Q is

torsion–free, then $gK = K$, so $g \in K$, hence, since K is torsion–free, $g = 1$, so G is torsion–free.

Now, let $G = \langle x,\ y \,|\, yxy^{-1} = x^{-1} \rangle$, then it is readily seen that G is an extension of $\mathbb{Z}$ ($\cong \langle x \rangle$) by $\mathbb{Z}$ ($\cong \langle y \rangle$) so it is torsion–free. But G can not be ordered since the positive cone of any total ordering on G has to contain either x or x^{-1} (by **PC1**), and hence both of them (by **PC3** and since $yxy^{-1} = x^{-1}$), which is impossible (by **PC1**). For abelian groups, the situation is much better: we shall show later (see theorem II.1.7, page 63) that an abelian group G can be ordered iff G is torsion–free.

It turns out that, for zero–divisor considerations, ordered group assumptions are unnecessarily stringent. A weaker condition is that of right ordered groups for which now we shall characterize their positive cones.

Proposition II.1.2 *A subset P of a group G is the positive cone of some right order of G iff it satisfies the following two conditions:*

RPC1. $G = P \coprod P^{-1} \coprod \{1\}$, *where* $\coprod$ *denotes the coproduct in the category of sets, i.e. "disjoint union",*

RPC2. $PP \subset P$,

Proof. This proof is similar to that of proposition II.1.1 above. If G is a r. o. group, then **RPC1** holds because $<$ is a linear order. Moreover, if $x,\ y \in P$, the $1 < y$, $1 < x$ only if $1 < y$, $y < xy$ so that $1 < xy$.

Conversely, if P satisfies **RPC1–2.** then $<$ is a linear order on G. Finally, if $x < y$ and $z \in G$, the $yx^1 \in P$ so that $(yz)(xz)^{-1} = yx^{-1} \in P$ and $xz < yz$. ∎

Theorem II.1.3 *Let k be a domain and $(G, ., <)$ be an ordered group. Then, $R = kG$ has only trivial units and is a domain.*

Proof. Consider a product $\alpha\beta$ where

$$\alpha = a_1 g_1 + \ldots + a_m g_m,\ g_1 < \ldots < g_m,\ a_i \neq 0\ (1 \leq i \leq m),$$
$$\beta = b_1 h_1 + \ldots + b_m h_m,\ h_1 < \ldots < h_m,\ b_i \neq 0\ \ (1 \leq i \leq n).$$

We have $g_1 h_1 \leq g_i h_j$, with equality iff $i = j = 1$. Thus, the "smallest" group element appearing in $\alpha\beta$ is $g_1 h_1$ (with non–zero coefficient $a_1 b_1$), and similarly the "largest" one is $g_m h_n$ (with non–zero coefficient $a_m b_n$). In particular, $\alpha\beta \neq 0$, and if $\alpha\beta = \beta\alpha = 1$, we must have $m = n = 1$, so $\alpha = a_1 g_1,\ \beta = b_1 h_1$, with $a_1 b_1 = b_1 a_1 = 1$ in k and $g_1 h_1 = 1$ in G. This proves that R is a domain, and that R has only trivial units. ∎

Lemma II.1.4 *Let S and T be two non–empty sets with T finite, and let $\mathcal{F}$ be a given family of functions from subsets of S to T satisfying the following two conditions.*

i. If $A \subset S$, $f : A \longrightarrow T$ and $B \subset A$, then $f_B \in \mathcal{F}$, where f_B denotes the restriction of f to B.

ii. For each finite subset $A \subset S$ there exists a function $f : A \longrightarrow T$ such that $f \in \mathcal{F}$.

Then, there exists a function $g : S \longrightarrow T$ such that $(g_A : A \longrightarrow T) \in \mathcal{F}$ for all finite subsets $A \subset S$.

Proof. First, to clarify matters, let's put the properties of $\mathcal{F}$ in words: $\mathcal{F}$ is a family of functions from S into T such that it contains all the restrictions of its elements and such that every finite subset of S is mapped to T by at least one function in $\mathcal{F}$.

Let $\mathcal{E}$ be the family of all those functions $(f : A \longrightarrow T) \in \mathcal{F}$, where A is a finite subset of S and such that for all finite subsets $B \supset A$ of S there exists a

function $(g : B \longrightarrow T) \in \mathcal{F}$ with $g_A = f$. In words, $\mathcal{E}$ is the family of functions of $\mathcal{F}$ with finite domain and which can be finitely extended by elements of $\mathcal{F}$.

We first check that $\mathcal{E} \neq \emptyset$ by showing that the empty function $\emptyset : \emptyset \longrightarrow T$ (i.e. the empty set) belongs to $\mathcal{E}$. Being the empty set a finite set included in S, and since the empty function is the unique function that maps the empty set to any set, then by ***ii.*** applied to the empty set, the empty function belongs to $\mathcal{F}$. Let $B \supset \emptyset$ be a finite subset of S. By ***ii.*** applied to B, there exists a function $(g : B \longrightarrow T) \in \mathcal{F}$. Since $g_\emptyset = \emptyset$, then, by definition of $\mathcal{E}$, the empty function belongs to $\mathcal{E}$. So, $\mathcal{E} \neq \emptyset$.

Let $\mathcal{H}$ be the family of all functions $f : D \longrightarrow T$, where $D \subset S$ and for all finite sets $A \subset D$ we have $f_A \in \mathcal{E}$. In words, $\mathcal{H}$ is the family of functions with domains included in S into T such that every finite restriction belongs to $\mathcal{E}$, i.e. (see the definition of $\mathcal{E}$ above) every finite restriction of any of its elements is finitely extendible by elements of $\mathcal{F}$. We check that $\mathcal{H} \neq \emptyset$ by showing that the empty function belongs to $\mathcal{H}$. We know that $\emptyset \subset S$. Since the only subset of $\emptyset$ is itself; $f_\emptyset = \emptyset$ and $\emptyset \in \mathcal{E}$, then $\emptyset \in \mathcal{H}$. So, $\mathcal{H} \neq \emptyset$ as well.

If $(f : D \longrightarrow T)$, $(g : E \longrightarrow T) \in \mathcal{H}$, then we define $f \leq g$ iff $D \subset E$ and $g_D = f$. Then, by a routine argument (which will be omitted), $\leq$ defines an order relation on $\mathcal{H}$. We check that $(\mathcal{H}, \leq)$ is an inductive set. Let $(\mathcal{C}, \leq)$ be a chain in $(\mathcal{H}, \leq)$. Let $F : U \longrightarrow T$, where $U = \bigcup \{A \,|\, (f : A \longrightarrow T) \in C\}$ and for all $(f : A \longrightarrow T) \in C$, $F_A = f$. Being $(\mathcal{C}, \leq)$ a chain, then by a routine argument (which will be omitted) F is well defined and is an upper bound for $(\mathcal{C}, \leq)$.

We show that $F \in \mathcal{H}$. To see this, we just need to check that every finite restriction of F belongs to $\mathcal{E}$. So, let $X \subset U$, X finite. We show that $F_X \in \mathcal{E}$. Note that since $(\mathcal{C}, \leq)$ is a chain in $(\mathcal{H}, \leq)$, then, in particular, the domains of the functions of $\mathcal{C}$ form a chain ordered by inclusion. Since X is **finite**, there must exists a set A such that $(f : A \longrightarrow T) \in \mathcal{C}$ and $X \subset A$ (the proof of this last claim is routine and will be omitted). Since $f \in \mathcal{C} \subset \mathcal{H}$; by definition, $\mathcal{H}$

contains all the finite restrictions of its elements so $f_X \in \mathcal{E}$ and by definition of F, $F_A = f$, then $F_X = f_X \in \mathcal{E}$. So, $F \in \mathcal{H}$.

Being $\mathcal{H}$ an inductive set, then, by Zorn's lemma, $\mathcal{H}$ contains a maximal element, say, $g : E \longrightarrow T$.

We now show that $E = S$ which will proved the lemma. Suppose not, assume that $E \neq S$ and choose $s \in S - E$. Then, $F := E \cup \{s\}$ properly contains E, and because T is finite, g extends to finitely many functions $(g_1 : F \longrightarrow T)$, $(g_2 : F \longrightarrow T)$, $\ldots$, $(g_n : F \longrightarrow T)$, where $n =$ card (T). Note that $g_i \notin \mathcal{H}$, for all $1 \leq i \leq n$, because if that were not the case, then g would not be maximal in $(\mathcal{H}, \leq)$. Thus, by definition of $\mathcal{H}$, for all $1 \leq i \leq n$, there exist finite subsets $A_i \subset F$ with $((g_i)_{A_i} : A_i \longrightarrow T) \notin \mathcal{E}$ and hence by definition of $\mathcal{E}$, for all $1 \leq i \leq n$, there exist finite subsets of S, call them B_i, such that $\mathbf{B_i \supset A_i}$ **and** $\mathbf{(g_i)_{A_i} : A_i \longrightarrow T}$ **does not extend to a function of** $\mathcal{F}$ **with domain** $\mathbf{B_i}$.

Let $A := \bigcup_{i=1}^{n}(E \cap A_i)$ and $B := \{s\} \cup \bigcup_{i=1}^{n} B_i$. Observe that A and B are subsets of S. Then, A and B are finite, since each A_i and B_i is finite and i runs from 1 up to n, where n is the finite cardinal of T (note that here is where we make essential use of the finiteness of T). Also, $A \subset E$ and $A \subset B$, by definition of A. Thus, since $g \in \mathcal{H}$, $g_A : A \longrightarrow T \in \mathcal{E}$, and hence, there exist a function of $\mathcal{F}$ that extends g_A to the finite set B, say, $f : B \longrightarrow T$, $f_A = g_A$. Note that by definition of A, by definition of F and since for all i, $A_i \subset F$ then for all i, $A_i \subset A \cup \{s\}$. Now, $s \in B$ and since $\{g_i(s)\}_{i=1}^{n} = T$ by the way the g_i where constructed, then since $f(s) \in T$, $f(s)$ must be equal $g_i(s)$, for some i. Hence for this particular i, we have $f_{A_i} = (g_i)_{A_i}$ because $A_i \subset A \cup \{s\}$, $f(s) = g_i(s)$ and $f_A = g_A$. Moreover, $B_i \subset B$ and since $f \in \mathcal{F}$, then by *i.* applied to B, we have that $(f_{B_i} : B_i \longrightarrow T) \in \mathcal{F}$. But $(g_i)_{A_i} = f_{A_i} = (f_{B_i})_{A_i}$, so for this particular i we got an extension of g_i to an element $f_{B_i} \in \mathcal{F}$, contradiction. So, $E = S$.

Therefore, $(g : S \longrightarrow T) \in \mathcal{H}$, so by definition of $\mathcal{H}$, for all finite $A \subset S$, $(g_A : A \longrightarrow T) \in \mathcal{E} \subset \mathcal{F}$. ∎

Let G be a group. If $x_1, x_2, \ldots, x_n \in G$, let us define $\mathbf{S(x_1, x_2, \ldots, x_n)}$ to be the subsemigroup of G generated by these elements, and similarly we let $\mathbf{S^G(x_1, x_2, \ldots, x_n)}$ to be the normal subsemigroup of G which they generate. In words, $S(x_1, x_2, \ldots, x_n)$ consists of all finite products of the form $x_{i_1}, x_{i_2}, \ldots, x_{i_j}$ with $j \geq 1$ and $S^G(x_1, x_2, \ldots, x_n)$ consists of all finite products of the form $x_{i_1}^{g_1}, x_{i_2}^{g_2}, \ldots, x_{i_j}^{g_j}$ with $j \geq 1$, where for all $x, g \in G$, $x^g := gxg^{-1}$.

Lemma II.1.5 *Let G be a group.*

i. *G is an r. o. group iff for all non-identity elements $x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in G$ there exist suitable signs $\varepsilon_i = \pm 1$ such that $1 \notin S(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$.*

ii. *G is an o. group iff for all non-identity elements $x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in G$ there exist suitable signs $\varepsilon_i = \pm 1$ such that $1 \notin S^G(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$.*

Proof. We shall consider the proof for ***ii.***, writting the similar remarks for ***i.*** between parenthesis; essentially, one needs to change $S(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$ by $S^G(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$ throughout.

Let G be an (right) ordered group with positive cone P and $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ be non-identity elements of G. Then, by **PC1.**, see page 54 (by **RPC1.**, see page 56), we can choose signs ε_i so that $1 < x_i^{\varepsilon_i}$. Then, with this choice, being the positive cone a normal subsemigroup $S^G(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n}) \subset P$ (in the case of r. o. group P is a subsemigroup by **RPC2**, and this is enough for $P \supset S(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$), and hence, by **PC1.** $1 \notin S^G(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$, (by **RPC1.** $1 \notin S(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n})$).

Now, we show the converse. Let $S = G - \{1\}$, let T be the finite set $T = \{1, -1\}$, and consider the family $\mathcal{F}$ of all functions $f : D \longrightarrow T$ from finite subsets D of S to T that satisfy the following condition, namely, if $D = \{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\}$, then

$$(f : D \longrightarrow T) \in \mathcal{F} \text{ iff } 1 \notin S^G$$

$(x_1^{f(x_1)}, x_2^{f(x_2)}, \ldots, x_n^{f(x_n)})$ $(1 \notin S(x_1^{f(x_1)}, x_2^{f(x_2)}, \ldots, x_n^{f(x_n)}))$. By assumption, the family $\mathcal{F}$ satisfies the conditions of lemma II.1.4, page 57, namely, it contains the restrictions of its elements and every finite subset of S is mapped to T by at least one function of $\mathcal{F}$. Hence, by that lemma, we conclude that there exists a function $g : S \longrightarrow T$ such that for all finite subsets $A \subset S$, $(g_A : A \longrightarrow T) \in \mathcal{F}$, where g_A notes the restriction of g to A. Let $P := \{x \in S \mid g(x) = 1\}$. We show that P defines a cone for G. Note, first, that if $x \in S$ then $g(x)$ and $g(x)^{-1}$ must have opposite signs. Indeed, if this were not the case, then we would have $1 = (1^{-1}x^{g(x)}1)(1^{-1}(x^{-1})^{g(x^{-1})}1) \in S^G(x^{g(x)}, (x^{-1})^{g(x^{-1})})$ $(1 = x^{g(x)}(x^{-1})^{g(x^{-1})} \in S(x^{g(x)}, (x^{-1})^{g(x^{-1})}))$ contradicting the properties of g. This shows that $P^{-1} = \{x \in S \mid g(x) = -1\}$ and, hence, $G = P \coprod P^{-1} \coprod \{1\}$, where $\coprod$ denotes the coproduct in the category of sets, i.e. "disjoint union". Finally, let $x, y \in P$ and let $z \in S^G(x, y) = S^G(x^{g(x)}, y^{g(y)})$ $(z \in S(x, y) = S(x^{g(x)}, y^{g(y)})$. Then, $z \neq 1$. Moreover, we must have $z \in P$; otherwise $g(z) = -1$ and $1 \in z^{-1}S^G(x, y) \subset S^G(x, y, z^{-1}) = S^G(x^{g(x)}, y^{g(y)}, z^{g(z)})$ $(1 \in z^{-1}S^G(x, y) \subset S^G(x, y, z^{-1}) = S^G(x^{g(x)}, y^{g(y)}, z^{g(z)}))$, which contradicts the fact that $g \in \mathcal{F}$. This shows that P is a normal subsemigroup (a semigroup) of G and proposition II.1.1, see page 54 (proposition II.1.2, see page 56) yields the result. ∎

The following are observations whose proofs will be omitted since they are routine to check, which will be used in the proof of the next lemma.

Observation 1: Suppose that A and B are ordered groups. Then, the group $A \times B$ becomes an ordered group by way of lexicographical ordering. By induction, it follows that every finite direct product of o. groups is an o. group (similarly for r. o. groups).

Observation 2: Let G be a group with subgroups H_1 and H_2, then $G/H_1 \cap H_2$ is embedded in $G/H_1 \times G/H_2$ by mapping $g+H_1 \cap H_2 \mapsto (g+H_1, g+H_2)$. By induction, this result can be extended to any finite number of subgroups H_i

of G (similarly for r. o. groups).

Observation 3: If G is an o. group or an r. o. group, then so is every subgroup of G with the induced order.

On the other hand, it is clear that this property is not inherited by quotients groups. Consider any free group G, by a result to be proved below (see theorem II.1.8), G is ordered, but moding out any relation of the form $g^n = 1$ for some $g \in G,\ n \in \mathbb{N}$, since $G/\langle g^n \rangle$ has torsion it can not be ordered (see page 55).

Lemma II.1.6 *Let G be a group.*

i. *If all finitely generated subgroups of G are o. groups (r. o. groups) then G is an o. group (r. o. group).*

ii. *If G has a family of normal subgroups H_ν such that $\bigcap_\nu H_\nu = \langle 1 \rangle$ and such that each quotient G/H_ν is an o. group (r. o. group) then G is an o. group (r. o. group).*

Proof. We consider only the case of o. groups, the results for r. o. groups being similar.

Now, suppose by way of contradiction that G is not an ordered group. Then, by lemma II.1.5 above, there exist non–identity elements $x_1,\ x_2,\ \ldots,\ x_n \in G$ such that $1 \in S^G(x_1^{\varepsilon_1},\ x_2^{\varepsilon_2},\ \ldots,\ x_n^{\varepsilon_n})$ for all 2^n choices of the signs $\varepsilon_i = \pm 1$.

Hence, the finitely generated subgroup $H := \langle x_1,\ x_2,\ \ldots,\ x_n \rangle$ of G has elements $x_1,\ x_2,\ \ldots,\ x_n$ such that $1 \in S^H(x_1^{\varepsilon_1},\ x_2^{\varepsilon_2},\ \ldots,\ x_n^{\varepsilon_n})$ for all choices of the signs, so, by lemma II.1.5 above, H can not be ordered, contradicting the assumption of ***i.***, so ***(i.)*** holds.

We now show ***ii.***. Because $\bigcap_\nu H_\nu = \langle 1 \rangle$, there exists a finite intersection $H = H_{\nu_1} \cap \ldots \cap H_{\nu_m}$ with $x_i \notin H$ for all i. If an over–bar denotes the homomorphism $G \longrightarrow G/H = \overline{G}$, then the foregoing shows that $\overline{x_i} \neq 1$, but since $1 \in S^G(x_1^{\varepsilon_1},\ x_2^{\varepsilon_2},\ \ldots,\ x_n^{\varepsilon_n})$ for all 2^n choices of sign, then $1 \in S^{\overline{G}}(\overline{x}_1^{\varepsilon_1},\ \overline{x}_2^{\varepsilon_2},\ \ldots,\ \overline{x}_n^{\varepsilon_n})$

for all choices of sign, hence $\overline{G}$ can not be ordered by lemma II.1.5. But, by observation 2 above, $\overline{G} = G/H$ is contained isomorphically in the finite direct product $\prod_{j=1}^{m} G/H_{v_j}$, and the latter is an o. group by assumption in ***ii.*** and observation 1, but this contradicts observation 3. So, ***ii.*** holds. ∎

In view of theorem II.1.3 (see page 56), it is of interest to know more examples of ordered groups.

Theorem II.1.7 *An abelian group G can be (right) ordered iff it is torsion-free.*

Proof. If G is (right) ordered then it must be torsion free (see page 55). Conversely, assume that the abelian group G is torsion-free. Let H be a finitely generated subgroup of G. Being H a finitely generated torsion-free abelian group then it is isomorphic to a finite direct product of copies of $\mathbb{Z}$. Being $\mathbb{Z}$ an (right) o. group, then, by observation 1 above, H can be (right) ordered. Hence, by lemma II.1.6, G can be (right) ordered. ∎

Theorem II.1.8 *Any free group can be ordered.*

Proof. Let G be a free group. We shall construct a positive cone on G. By the Magnus–Witt theorem (see Magnus, Karras and Solitar [MKS76], Sec 5.7; or Huppert and Blackburn [HB82], pp. 380–383) for the lower central series[1] of G, $G \supset G^{(1)} \supset G^{(2)} \supset G^{(3)} \supset \ldots$, we have that $\bigcap_{n\in\mathbb{N}} G^{(n)} = \{1\}$, and each $G^{(n)}/G^{(n+1)}$ is free abelian (in particular they are torsion-free abelian). Hence, by theorem II.1.7, for all $n \in \mathbb{N}$, $G^{(n)}/G^{(n+1)}$ can be ordered. Let P_n be a positive cone in $G^{(n)}/G^{(n+1)}$ defining on it the structure of an ordered abelian group. Now let P be the subset of G consisting of all elements $g \neq 1$ with the property that, if n is the (unique) integer such that $g \in G^{(n)} \backslash G^{(n+1)}$ then the coset $gG^{(n+1)}$ belongs to P_n. We have that G is the disjoint union of $\{1\}$, P and P^{-1}. We also have that, for any $z \in G$, $z^{-1}Pz \subseteq P$, for, if $g \in G$ is such

[1] $G^{(1)} := [G,\ G]$ (the commutator group) and for all $n \in \mathbb{N}$, $G^{(n+1)} := [G,\ G^{(n)}]$

that $g \in G^{(n)} \backslash G^{(n+1)}$ and $gG^{(n+1)} \in P_n$, then $z^{-1}gz \in G^{(n)} \backslash G^{(n+1)}$ and

$$z^{-1}gz = g.g^{-1}z^{-1}gz \in g.[G, G^{(n)}] = gG^{(n+1)},$$

so $z^{-1}gzG^{(n+1)} \in P_n$. To complete the proof that P is a positive cone on G, it only remains to show that $P.P \subseteq P$. Let g, h be elements in P, with

$$g \in G^{(n)} \backslash G^{(n+1)},\ h \in G^{(m)} \backslash G^{(m+1)},\ \text{and}$$
$$gG^{(n+1)} \in P_n,\ hG^{(m+1)} \in P_m.$$

To show that $gh \in P$, we may assume that $m \geq n$. If $m > n$, then $h \in G^{(m)} \subseteq G^{(n+1)}$; in this case $gh \in G^{(n)} \backslash G^{(n+1)}$ and

$$ghG^{(n+1)} = gG^{(n+1)} \in P_n,$$

so by definition $gh \in P$. If $m = n$, then $gG^{(n+1)}$, $hG^{(n+1)} \in P_n$ show that $ghG^{(n+1)} \in P_n$; in particular, $gh \in G^{(n)} \backslash G^{(n+1)}$, so again $gh \in P$. ∎

II.2 The Malcev–Neumann construction

There is an important generalization of the power series method, to which we now turn. Let G be a group and consider the group algebra kG over a commutative field k. When is kG embeddable in a skew field?. Clearly, a necessary condition is that it should be entire, and for this it is necessary for G to be torsion free. For if $u \in G$ is of order n, then

$$(u-1)(u^{n-1} + u^{n-2} + \ldots + u + 1) = 0.$$

In the abelian case this condition on G is also sufficient. For if G is torsion free abelian, it can be totally ordered (c.f. theorem II.1.7, page 63). When G

is ordered then, by theorem II.1.3 (see page56), kG is a domain, and being a commutative ring, it is embeddable in a field, hence we have

Theorem II.2.1 *Let G be an abelian group, then the group algebra kG (over any commutative field k) is embeddable in a field iff G is torsion free.* ∎

In the non–commutative case little is known; it is not even known whether kG is entire for any torsion free G. But Farkas and Snider [FS76] have proved that this is the case when G is **polycyclic** (i.e. soluble with maximum condition on subgroups); since kG is noetherian in this case, it is then embeddable in a field. Also, Lewin and Lewin [LL77] have shown that for any torsion free group G with a single defining relation the group algebra kG can be embedded in a skew field.

It has long been known that theorem II.2.1 can be generalized to non–abelian groups which are ordered. In that case we can form a kind of power series ring $k((G))$ which turns out to be a skew field.

In order to present the Malcev–Neumann construction we shall need the following characterization of well ordered subsets of a totally ordered set.

Lemma II.2.2 *Let $(G, <)$ be a totally ordered set. For any subset $S \subset G$, the following are equivalent:*

(1) *S is well ordered.*

(2) *S satisfies **DCC**[2] (i.e. any sequence $s_1 \geq s_2 \geq s_3 \geq \dots$ in S is eventually constant: there exists $j \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $n \geq j$, $s_n = s_j$).*

(3) *Any sequence $\{s_1, s_2, s_3, \dots\}$ in S contains a subsequence $\{s_{n_1}, s_{n_2}, s_{n_3}, \dots\}$ (where $n_1 < n_2 < n_3 < \dots$) such that $s_{n_1} \leq s_{n_2} \leq s_{n_3} \leq \dots$.*

[2] *descending chain condition (on sequences).*

Proof. (3) only if (2): let

$$(*) \qquad s_1 \geq s_2 \geq s_3 \geq \dots$$

in S. By (3), there exist a subsequence $s_{n_1} \leq s_{n_2} \leq s_{n_3} \leq \dots$ such that $n_1 < n_2 < n_3 < \dots$. Then, we claim that for all $n \geq n_1$, $s_n = s_{n_1}$, proving (2). Indeed, if $n \geq n_1$ then by $(*)$ $s_{n_1} \geq s_n$. If $s_{n_1} > s_n$, take any $n_i > n$ in the subsequence, since $n_1 < n_i$ then $s_{n_1} \leq s_{n_i}$, so $s_{n_i} > s_n$ and $n_i > n$ contradicting $(*)$. So, $s_n = s_{n_1}$.

(2) only if (1): suppose S is not well ordered. Then, there exist a non–empty subset T of S such that T does not have a least element. Being T non–empty, let $t_1 \in T$; since T fails to have a least element, then there must exist $t_2 \in T$ such that $t_1 > t_2$, since T fails to have a least element, then there must exist $t_3 \in T$ such that $t_2 > t_3$, ..., contradicting (2). So, (1) holds.

(1) only if (3): Let $\{s_1, s_2, s_3, \dots\}$ be a sequence in a well ordered subset S of G. Take n_1 such that $s_{n_1} = \min\{s_i : i \geq 1\}$. Then, take $n_2 > n_1$ so that $s_{n_2} = \min\{s_i : i > n_1\}, \dots$, etc. This produces a non–decreasing subsequence $s_{n_1} \leq s_{n_2} \leq s_{n_3} \leq \dots$, as desired. So, (3) holds. ∎

Lemma II.2.3 *Let S, T be well ordered subsets of a totally ordered set $(G, <)$.*

(1) *$S \cup T$ is well ordered.*

(2) *If $(G, <)$ is an ordered group, then $U := S.T = \{st : s \in S,\ t \in T\}$ is also well ordered. Moreover, for any $u \in U$, there exist only a finite number of ordered pairs (s, t) $(s \in S,\ t \in T)$ such that $u = st$.*

Proof. (1) Let A be a non–empty subset of $S \cup T$. If $S \cap A = \emptyset$ then $A \subset T$, so, A has a least element since T is well ordered. Similarly, if $T \cap A = \emptyset$. So, assume $S \cap A \neq \emptyset \neq T \cap A$. Note that $S \cap A$ is a non–empty subset of the well ordered set S, so it has a least element. Similarly, $T \cap A$ has a least element. It

is routine to check (the proof will be omitted) that min $\{\min S \cap A, \min T \cap A\}$ is the least element of A. So, (1) holds.

(2) Assume that U is not well ordered. By lemma II.2.2 above, there would exist a strictly decreasing sequence $s_1t_1 > s_2t_2 > \cdots$ where $s_i \in S$ and $t_i \in T$. After replacing $\{s_1, s_2, \ldots\}$ by a subsequence, we may assume, since S is well ordered, that $s_1 \leq s_2 \leq s_3 \leq \cdots$. If $t_i \leq t_{i+1}$ for some i, we would have $s_it_i \leq s_{i+1}t_i \leq s_{i+1}t_{i+1}$, contradiction. Thus we must have $t_1 > t_2 > t_3 > \cdots$. But this contradicts the fact that T is well ordered. So, U must be well ordered.

To see the "moreover" part, suppose by way of contradiction that there is a $u \in U$ such that there exist an infinite set $\mathcal{U} := \{(s, t) \in S \times T : st = u\}$. Choose a countable subset of $\mathcal{U}$ like $\mathcal{N} := \{(s_i, t_i) \in \mathcal{U} : i \in \mathbb{N}$ and for all $i, j \in \mathbb{N}$, $i \neq j$, $(s_i, t_i) \neq (s_j, t_j)\}$. If $\mathcal{S} := \{s_i \in S : i \in \mathbb{N}$ and $(s_i, t_i) \in \mathcal{N}\}$ is finite, since $t_i = s_i^{-1}u$ then $\mathcal{T} := \{t_i \in T : i \in \mathbb{N}$ and $(s_i, t_i) \in \mathcal{N}\}$ will be finite as well, contradicting the fact that $\mathcal{N}$ is infinite. So, we may assume that $\mathcal{S}$ is infinite. Since S is well ordered and infinite, we may assume, replacing S by a subsequence if necessary, that the elements of $\mathcal{S}$ verify $s_1 < s_2 < s_3 < \cdots$. If $t_i \leq t_{i+1}$ for some i, we would have $u = s_it_i < s_{i+1}t_i < s_{i+1}t_{i+1} = u$, contradiction. Thus we must have $t_1 > t_2 > t_3 > \cdots$. But this contradicts the fact that T is well ordered. So, such a u can not exist. ∎

We are now ready to present the general Malcev–Neumann construction of formal a power series ring. For this end, we fix a base ring R and an ordered group $(G, <)$. We assume that G is multiplicatively written, and write $P = \{x \in G : x > 1\}$ for the positive cone of the ordering on G. Furthermore, we fix a group homomorphism ω from G to $Aut(R)$, the group of automorphisms of the ring R; the image of $g \in G$ under ω will be denoted by ω_g.

As a set, the Malcev–Neumann ring $A = R((G, \omega))$ consists of certain formal, but not necessarily finite, sums

$$\alpha = \sum_{g \in G} \alpha_g g \quad (\text{"formal power series"})$$

where the α_g's are elements of R. By a **formal power series** $\alpha = \sum_{g \in G} \alpha_g g$ we mean a function $\alpha : G \longrightarrow R$ defined for all $g \in G$ by $\alpha(g) = \alpha_g$. For each such α, we define the **support** of α by $supp(\alpha) := \{g \in G : \alpha_g \neq 0\}$.

Now we define

$$\text{(II.1)} \quad A = R((G, \omega)) = \left\{\alpha = \sum \alpha_g g : supp(\alpha) \subset G \text{ is well ordered}\right\}.$$

In A, we add and multiply elements according to the following formal rules:

$$\text{(II.2)} \qquad \sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g,$$

$$\text{(II.3)} \qquad \left(\sum_{g \in G} \alpha_g g\right) \cdot \left(\sum_{h \in G} \beta_h h\right) = \sum_{u \in G} \left(\sum \alpha_g \omega_g (\beta_h)\right) u,$$

where the last sum is over all (g, h) such that $gh = u$. Since we agree, as usual, that a sum with infinitely many sums equal to zeros is equal to zero, we may restrict g and h respectively to $supp(\alpha)$, $supp(\beta)$, and these supports are well ordered sets in G, the last sum (II.3) is finite by II.2.3. Also, since

$$supp(\alpha + \beta) \subset supp(\alpha) \cup supp(\beta),$$
$$supp(\alpha\beta) \subset supp(\alpha).supp(\beta),$$

the supports on the LHS are both well ordered by (II.2.3). Therefore, addition and multiplication are well–defined in A. Having made this observation, it is straightforward to check (the proof will be omitted) that $(A, +, .)$ is a ring.

The subring of A consisting of all **finite sums** $\alpha = \sum \alpha_g g$ (i.e. sums of finite support) is called the **twisted group ring** $R * G$ which we denote $R[G, \omega]$. As usual, we shall identify R with the subring $R.1 \subset A$, and identify G with the subgroup $1.G$ of invertible elements in A. If ω happens to be the trivial homomorphism, the resulting **untwisted ring of formal power series** will be denoted $R((G))$.

The idea of multiplying two "series" α and β by (II.3) stems from the distributive law and the twist law $g.r = \omega_g(r)g$, where $r \in R$ and $g \in G$. In the special case when G is an infinite cyclic group $\{x^n : n \in \mathbb{Z}\}$ ordered by the positive cone $P = \{x^n : n > 0\}$, the homomorphism $\omega : G \longrightarrow Aut(R)$ is specified by a single automorphism $\sigma := \omega_x$. In this case, the twist law boils down to $x.r = \sigma(r)x$ (for $r \in R$), and

$$A = R((\langle x \rangle, \omega)) = \left\{ \sum_{i=n}^{\infty} \alpha_i x^i : \ \alpha_i \in R, \ n \in \mathbb{Z} \right\}$$

is just the **Hilbert's twisted Laurent series ring** $R((x, \sigma))$ (see page 45), noting that well ordered subsets of $\mathbb{Z}$ are just non–empty subsets which are bounded below.

In the ordered group (G, P), we shall now classify the elements of P according to their "archimedean" character. Let $s, t \in P$. If $s^n < t$ for all $n \in \mathbb{N}$, we call s **infinitely smaller** than t and write $s \ll t$ or $t \gg s$. We also call t **infinitely larger** than s. We say that two elements s and t in P are **relatively archimedean** (written $s \sim t$) if $s \leq t^m$ and $t \leq s^n$ for some $m, n \in \mathbb{N}$. It is routine to check (the proof will be omitted) that "$\sim$" is an equivalence relation on P. The equivalence class of $s \in P$ will be denoted by $[s]$, which is called the **archimedean class** of s. Given two archimedean classes $[r]$ and $[s]$, we define $[r] < [s]$ if $r^n < s$ for all $n \in \mathbb{N}$. It is routine to check (the proof will be omitted) that "$<$" is well defined (independently of the choice of the class representatives), and gives a *total* ordering on the set of all the archimedean

classes of G. As usual, we define $[r] \leq [s]$ to mean either $[r] < [s]$ or $[r] = [s]$.

Lemma II.2.4 *The archimedean class of a product is the class of the greatest factor, i.e., for any elements $s_1, \cdots, s_n \in P$, we always have*

$$[s_1 \cdots s_n] = [max\{s_1, \ldots, s_n\}].$$

Proof. If, say $s_i = max\{s_1, \ldots, s_n\}$, then $s_1 \cdots s_n \leq s_i^n$ and $s_i \leq s_1 \cdots s_n$ (since all $s_j > 1$). This shows that $s_i \sim s_1 \cdots s_n$, and so $[s_1 \cdots s_n] = s_i$. ∎

The following lemma is the crux of the Malcev–Neumann embedding.

Lemma II.2.5 *Let S be a well ordered subset of P in the ordered group (G, P). Let $S^n = \{s_1 \cdots s_n : s_i \in P\}$ for $n \geq 1$, and let $S^\infty = \bigcup_{n \geq 1} S^n \subset P$. Then*

(1) *S^∞ is well ordered.*

(2) *Any $u \in S^\infty$ lies in only finitely many S^n's.*

Proof. (1) Assume that S^∞ is not well ordered. Then, by lemma II.2.2 (see page 65), there exists a strictly decreasing sequence $u_1 > u_2 > \cdots$ in S^∞, say $u_i = s_{i1} s_{i2} \cdots s_{in_i}$, where $s_{ij} \in S$. We claim that the sequence of archimedean classes $[u_1] \geq [u_2] \geq \cdots$ is eventually constant. To see this, let $s_i = max\{s_{i1}, \ldots, s_{in_i}\} \in S$. By lemma II.2.4, $[u_i] = [s_i]$ so we have $[s_1] \geq [s_2] \geq \cdots$. Since $\{s_1, s_2, \cdots\} \subset S$ has a smallest element, say s_{i_0}, the sequence $[s_1] \geq [s_2] \geq \cdots$ must stabilize after i_0 terms, as claimed.

Let $U := min\{[u_i] : i \geq 1\} = [s_{i_0}]$. A different choice of a strictly decreasing sequence in S^∞, say $u_1' > u_2' > \cdots$, would lead to another archimedean class U'. Since any such class is the class of an element in S, we may assume that our initial $u_1 > u_2 > \cdots$ has been chosen such that U is as small as possible. After discarding a finite number of u_i's, we may assume that $U = [u_i] = [s_i]$ for all $i \geq 1$.

Consider the set $\mathcal{U} := \{s \in S : [s] = U\}$, it is non–empty since s_{i_0} belongs to it. Since $\mathcal{U} \subset S$, it has a least element, say s_U. Since $[s_U] = [u_1]$, there exists an integer $m \geq 1$ such that $u_1 \leq s_U^m$. We may further assume that the sequence (subject to all foregoing restrictions) has been so choosen that the m we took above is as small as possible. We represent each u_i in one of the following four forms:

$$u_i = \begin{cases} s_i \\ v_i s_i \\ s_i w_i \\ v_i s_i w_i \end{cases}$$

where v_i, $w_i \in S^\infty$. Only a finite number of the u_i's can be of the first type, for otherwise we would have a strictly decreasing sequence in S, contradicting the fact that S is well ordered. Therefore, there must exist a sequence of the u_i's of one of the other three types, say, the fourth type. (The other two types are similar). After passing to a subsequence, we may assume that $u_i = v_i s_i w_i$ for all i. Let $B = \{v_i : i \geq 1\}$, $C = \{w_i : i \geq 1\}$ and let $D = \{s_i : i \geq 1\} \subset S$. If B and C are both well ordered, then by applying two times lemma II.2.3 (see page 66), BDC is also well ordered, and $u_1 > u_2 > \cdots$ in BDC gives a contradiction. Thus, we may assume, say, B is not well ordered. After replacing the v_i's by a subsequence, we may therefore assume that $v_1 > v_2 > \cdots$ in $B \subset S^\infty$. We have seen earlier that $V := min\{[v_i] : i \geq 1\}$ exists, and, since $v_i \leq u_i$ (because $s_i w_i > 1$), we have $V \leq U$. By the minimal choice of U, we get $V = U$ (and hence $s_V = s_U$). As before, we may assume that $[v_1] = [v_2] = \cdots$. From $v_1 s_U \leq v_1 s_1 \leq v_1 s_1 w_1 = u_1 \leq s_U^m$, we see that $m \geq 2$ (for otherwise $v_1 \leq 1$). But then cancellation of s_U shows that $v_1 \leq s_U^{m-1} = s_V^{m-1}$, so $v_1 \leq s_V^{m-1}$, this contradicts the minimal choice of m.

(2) Assume that there is a counterexample to (2). Since S^∞ is well ordered by (1), there exists a least counterexample $u \in S^\infty$. For $1 \leq i < \infty$,

write $u = s_{i1}s_{i2}\cdots s_{in_i}$ where $2 \leq n_1 < n_2 < \cdots$, and $s_{ij} \in S$. Since $u = s_{i1}.(s_{i2}\cdots s_{in_i}) \in S.S^{\infty}$, and both S and S^{∞} are well ordered, (II.2.3) the "moreover" part shows that there is an element $v \in G$ such that $s_{i2}\cdots s_{in_i} = v$ for infinitely many i's. Then, this v lies in infinitely many S^n's, but since $s_{i1} > 1$ (for all i), we have, by multiplying with $(s_{i2}\cdots s_{in_i})$, $u > v$. This contradicts the choice of u as the least counterexample. ∎

Note that by lemma (II.2.3) and induction, we know that each S^n $(n \geq 1)$ is well ordered.

Corollary II.2.6 *Let $\alpha \in \sum \alpha_g g \in A = R((G,\omega))$ be such that $S := supp(\alpha)$ lies in P. Then for any $a_0, a_1, \cdots \in R$, the sum*

$$\gamma = a_0 + a_1\alpha + a_2\alpha^2 + \cdots \in A.$$

Proof. Since $supp(\alpha^n) \subset S^n$, each $g \in G$ can lie in $supp(\alpha^n)$ only for finitely many n's, according to lemma II.2.5 part (2). Therefore, the sum $\gamma = a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ is well defined. Furthermore, $supp(\gamma)$ is well ordered since it lies in

$$\{1\} \cup \bigcup_{n\geq 1} S^n = \{1\} \cup S^{\infty}.$$

Therefore, $\gamma \in A$. ∎

The reason we are interested in $R((G,\omega))$ in this section is given in the next theorem. Observe that in this result, no additional assumption on the homomorphism $\omega : G \longrightarrow Aut(R)$ is needed.

Theorem II.2.7 *Assume R is a division ring, $(G,<)$ an ordered group. We assume that G is multiplicatively written, and write $P = \{x \in G : x > 1\}$ for the positive cone of the ordering on G. Furthermore, we fix a group homomorphism ω from G to $Aut(R)$, the group of automorphisms of the division ring R.*

Then $A = R((G,\omega))$ is also a division ring.

Proof. Consider a non–zero element $\beta = \sum \beta_g g \in A$. Let g_0 be the least element in $supp(\beta)$. Then, $\beta_{g_0}^{-1} . \beta . g_0^{-1} = 1 - \alpha$ where $\alpha \in A$ has $supp(\alpha) \subset P$. By corollary II.2.6,

$$\gamma = 1 + \alpha + \alpha^2 + \cdots$$

is a well–defined element of A, and a routine formal check (which will be omitted) shows that γ is an inverse of $1 - \alpha$. Therefore, $1 - \alpha$ is a unit in A, and so $\beta = \beta_{g_0}(1 - \alpha)g_0$ is also a unit in A. ∎

Corollary II.2.8 *Let R be any division ring, and $(G, <)$ and ω be as in the theorem. Then, the twisted group ring $R[G, \omega]$ can be embedded in a division ring, namely $R((G, \omega))$.* ∎

Let I be any non–empty set and $\{x_i : i \in I\}$ be a set of independent indeterminates each of which commutes with R. The free ring $R\langle x_i : i \in I\rangle$ generated by $\{x_i\}$ over R is a subring of the group ring $R[G]$, where G is the free group generated by $\{x_i\}$. Since by theorem II.1.8 (see page 63) any free group can be ordered, we have the following consequence of corollary II.2.8 by taking ω to be the trivial homomorphism.

Corollary II.2.9 *For any division ring R, the free ring*

$$R\langle x_i : i \in I \text{ and } x_i \text{ commutes with } R\rangle$$

can be embedded in a division ring. ∎

It is then clear that $k\langle X\rangle$, the free k–algebra on a set X over a commutative field k, can be embedded in kF, the group algebra of the free group on X, and since kF is embedded in the formal power series division ring $k((F))$, we have an embedding of $k\langle X\rangle$ in a skew field. If instead of the free group F we take the **free metabelian group** G, i.e. the group defined by the law $((u, v), ((w, x)) = 1$, where $(x, y) = x^{-1}y^{-1}xy$, by Moufang's theorem [Mou37], we can still embed

$k\langle X\rangle$ in kG, at least when $card(X) = 2$. Moreover, G can again be ordered (c.f. [Mou37]), so we have another embedding of $k\langle X\rangle$ in a division ring, and these two embeddings of $k\langle X\rangle$ in $k((F))$ and $k((G))$ are distinct, c.f. Moufang (loc. cit.).

Let us now consider Hilbert's example (see page 45 and page 69). Let k be a commutative field, and σ be a fixed automorphism of k. We write $D = k((x, \sigma))$ for the ring of formal Laurent series $\sum_{i=n}^{\infty} a_i x^i$, where $n \in \mathbb{Z}$ and $a_i \in k$, with multiplication defined by the twist equation $xa = \sigma(a)x$ (for all $a \in k$). By comment made in page 69 and theorem II.2.7 we know D is a division ring. The following proposition computes the center $Z(D)$ of D and determines, in particular, when D is centrally finite.

Proposition II.2.10 *For $D = k((x, \sigma))$ as above, let $k_0 \subset k$ be the fixed field of σ; i.e. $k_0 = \{a \in k : \sigma(a) = a\}$. Then*

$$Z(D) = \begin{cases} k_0 & \text{if } \sigma \text{ has infinite order,} \\ k_0((x^s)) & \text{if } \sigma \text{ has finite order } s. \end{cases}$$

In particular, the division ring D is centrally finite iff σ has finite order.

Proof. Consider a series $f = \sum_{i=n}^{\infty} a_i x^i \in Z(D)$, and let j be an index such that $a_j \neq 0$. For any scalar $a \in k$, we have $(\sum a_i x^i)a = a(\sum a_i x^i)$, so, comparing the coefficients for x^j, we get $a_j \sigma^j(a) = a a_j$; hence $\sigma^j(a) = a$.

Case 1. *σ has infinite order.* In this case, the above argument shows that $a_j \neq 0$ is only possible for $j = 0$. Hence $f = a_0$. Since we also have $a_0 x = x a_0 = \sigma(a_0)x$, it follows that $\sigma(a_0) = a_0$; i.e., $a_0 \in k_0$. Conversely, any $a_0 \in k_0$ clearly commutes with any power series, so $Z(D) = k_0$. Since $dim_{k_0} D$ is clearly infinite (indeed, $\{x^i : i \in \mathbb{N}\}$ is linearly independent over k_0), D is not centrally finite in this case.

Case 2. *σ has finite order s.* The first paragraph of the proof shows that if $a_j \neq 0$ in a series $f = \sum_{i=n}^{\infty} a_i x^i \in Z(D)$, then $\sigma^j = 1_k$, so s divides j. But we also have $fx = xf$, which shows that each $a_i \in k_0$. thus $f \in k_0((x^s))$ (the ordinary Laurent series field in x^s over k_0). Conversely, it is easy to verify that any monomial ax^{sj} with $a \in k_0$ commutes with any series in D, so $Z(D) = k_0((x^s))$. Let $F = k_0((x^s))$ and $K = k((x^s))$. Since x^s commutes with all elements of k, K is again the ordinary Laurent series field in x^s over k. We have $dim_F K = dim_{k_0} k = s$ by Galois theory (actually, by Artin's theorem, see [Hun89], page 252), and, since

$$D = K.1 \oplus K.x \oplus \cdots \oplus K.x^{s-1},$$

the dimension of D as a left K–vector space is also s. By the transitivity formula for dimensions, it follows that $dim_{Z(D)} D = dim_F D = s^2$. In particular, D is a centrally finite division ring. ∎

The following corollary follows from the argument in the proof of Case 1 in proposition II.2.10.

Corollary II.2.11 *If R is a field, $(G, <)$ is a nontrivial ordered group, $\omega : G \longrightarrow Aut(R)$ is an injective homomorphism and $A := R((G, \omega))$, then*

$$Z(A) = R^G := \{r \in R : \ \omega_g(r) = r \text{ for all } g \in G\},$$

and the division ring A is centrally infinite. ∎

II.3 Examples of non–left Ore rings embeddable in fields

We have as a corollary of theorem II.2.7 (see page 72) that the group ring of a free group can be embedded in an ordered division ring. We now show that the

Ore criterion (see theorem I.3.8, page 23) does not apply to the group ring of a free group of, let us say, two generators.

Let F be the free group generated by two elements a, b; for the purpose of this section it need not be ordered (however, c.f. theorem II.1.8, page 63). We use the "length" of an element of F: if

$$g = \prod_{v=0}^{n} a^{\alpha_v} b^{\beta_v} \in F, \text{ where } \begin{cases} \alpha_v \in \mathbb{Z},\ \alpha_v \neq 0,\ v = 1, \dots, n, \\ \beta_v \in \mathbb{Z},\ \beta_v \neq 0,\ v = 0, \dots, n-1, \end{cases}$$

then

$$\lambda(g) = \sum |\alpha_v| + |\beta_v|$$

is called the **length** of g. The unit element has zero length by definition. Let X and Y be subsets of F, by XY we denote the subset of F of all products xy, $x \in X$, $y \in Y$; and the element x and the subset $\{x\} \subset F$ will not be distinguished.

Lemma II.3.1 *Let X and Y be subsets of F, not both empty, and let*

$$(X \cup Xa) - (X \cap Xa) \subset Y \cup Yb, \tag{II.4}$$

$$(Y \cup Yb) - (Y \cap Yb) \subset X \cup Xa. \tag{II.5}$$

Then, X or Y is infinite.

Proof. We may assume X finite but not empty. Then $X \cup Xa$ is also finite and not empty. Let g be an element in $X \cup Xa$ of maximal length, and consider the elements

$$g_1 := ga, \quad g_2 = ga^{-1}. \tag{II.6}$$

As g lies in X or in Xa, g_1 lies in Xa, or g_2 lies in X: in any case one of the two lies in $X \cup Xa$. Hence $\lambda(g_1) \leq \lambda(g)$ or $\lambda(g_2) \leq \lambda(g)$. However, definition (II.6)

shows that $\lambda(g_i) = \lambda(g) \pm 1$, the negative sign applying only when the last generator of g is cancelled by the $a^{\pm 1}$. Hence, g must end in a (positive or negative) power of a.

Also either $\lambda(g_1) = \lambda(g) + 1$ or $\lambda(g_2) = \lambda(g) + 1$, so that either g_1 or g_2 does not lie in $X \cup Xa$ by the maximality of the length of g. Hence, g can not lie in both X and Xa, and we see that

$$g \in (X \cup Xa) - (X \cap Xa);$$

thus by (II.6) also $g \in Y \cup Yb$.

Therefore, any element of maximal length in $X \cup Xa$ ends in $a^{\pm 1}$ and also lies in $Y \cup Yb$. The symmetry of the assumptions then shows that such an element can not be of maximal length in $Y \cup Yb$, because it does not end in $b^{\pm 1}$; and no longer element can be of maximal length in $Y \cup Yb$ because it could not lie in $X \cup Xa$; $Y \cup Yb$ has no element of maximal length, but is not empty either. Therefore $Y \cup Yb$ is infinite, and so then is Y. ∎

Theorem II.3.2 *Let K be a ring, F the free group of two free generators a, b, and KF the group ring of F over K. Then, the elements*

(II.7) $$\alpha := 1 + a; \quad \beta := 1 + b$$

have no common (nontrivial) left multiple in KF.

Proof. Assume that

(II.8)

$$\xi\alpha = \eta\beta = \zeta, \text{ where } \begin{cases} \xi = \sum_{i=1}^{n} k_i f_i, \ n \in \mathbb{N}, \ k_i \in K, \ f_i \in F, \\ \eta = \sum_{j=1}^{m} k_j g_j, \ m \in \mathbb{N}, \ k_j \in K, \ g_j \in F \text{ and} \\ \zeta = \sum_{l=1}^{s} k_l h_l, \ l \in \mathbb{N}, \ k_l \in K, \ h_l \in F, \end{cases}$$

are elements of the group ring KF. We may here assume that all coefficients

are non–zero. Denote by

$$X = \{f_i\}_{i=1}^{n}, \quad Y = \{g_j\}_{j=1}^{m}, \quad Z = \{h_l\}_{l=1}^{s}.$$

Then, by (II.7) and (II.8) we clearly have

$$(X \cup Xa) - (X \cap Xa) \subset Z \subset X \cup Xa$$

and also

$$(Y \cup Yb) - (Y \cap Yb) \subset Z \subset Y \cup Yb.$$

Hence, lemma II.3.1 applies; and as X and Y are finite, they must be empty. Then $\xi = \eta = 0$ and then $\zeta = 0$, so the only common left multiple of α and β is trivial. This proves the theorem and shows that the Ore criterion does not apply to the group ring (over any coefficient ring) of the free group. ∎

II.4 Complete topological groups

Since in the proof of Cohn's embedding theorem (see section II.6, page 91) we shall make essential use of the concept and basic properties of a complete topological group which is regular, it will be convenient to present at this point the definitions and theorems we shall need. For complete expositions of this subject see Bourbaki [Bou74], Higgins [Hig74], Husain [Hus66], Warner [War89].

A topology τ on a group G is a **group topology**, and G, furnished with τ, is a **topological group** if

TG 1 $(x, y) \mapsto xy$ is a continuous map from $G \times G$, furnished with the Cartesian product topology defined by $\mathcal{T}$, to G;

TG 2 $x \mapsto x^{-1}$ is a continuous map from G to G.

A **topological group morphism** $f : G \longrightarrow H$, where G, H are topological groups is a continuous group homomorphism.

Any subgroup H of a topological group G is a topological group with respect to the induced topology and the inclusion $j : H \hookrightarrow G$ is a morphism of topological groups.

A basic principle. Let G be a topological group and let g be a fixed element of G. The constant map $x \mapsto g$ and the identity map $x \mapsto x$ are continuous maps from G to G, so they induce a continuous map $x \mapsto (g, x)$ from G to $G \times G$. Composing this with the continuous multiplication $G \times G \longrightarrow G$ we get a continuous map $l_g : x \mapsto gx$ from G to G, called **left multiplication** (or **left translation**) by g. This map has inverse $l_{g^{-1}}$ which is also continuous, so l_g is a **homeomorphism** $G \longrightarrow G$ (i.e. a topological isomorphism; but it is not a topological group isomorphism). Similarly, all right translations $r_g : x \mapsto xg$ are homeomorphisms $G \longrightarrow G$. Moreover, the conjugations maps $x \mapsto gxg^{-1}$ are topological group isomorphisms (routine verification). As a consequence G must be a **homogeneous space**, that is, given $a, b \in G$ there is a homeomorphism $G \longrightarrow G$ sending a to b ($l_{ba^{-1}}$ or $r_{a^{-1}b}$ will do). Thus, **G looks topologically the same at all points**. We can now use translations to transfer topological information from one point to another in any topological group, and this basic method is used in almost every proof in the subject.

If f_1 and f_2 are functions respectively from sets S_1 to T_1 and from S_2 to T_2, we denote by $f_1 \times f_2$ the function $(s_1, s_2) \mapsto (f(s_1), f_2(s_2))$ from $S_1 \times S_2$ to $T_1 \times T_2$.

The following theorem gives a useful alternative criterion for a topology on a group to be a group topology.

Theorem II.4.1 *A topology τ on a group G is a group topology iff*

TG 3 *$(x, y) \longrightarrow xy^{-1}$ is continuous from $G \times G$, furnished with the Cartesian product topology defined by τ, to G.*

Proof. Let m, j and q be respectively the functions of $(TG1)$, $(TG2)$ and $(TG3)$, and let $i_2 : G \longrightarrow G \times G$ be the continuous function defined by $i_2(y) := (1, y)$ for

all $y \in G$. The condition is necessary, since $q = m \circ (id_G \times j)$, and sufficient, since $j = q \circ i_2$ and $m = q \circ (id_G \times j)$. ∎

If A and B are subsets of a group G, we write AB for $\{xy \in G : x \in A, y \in B\}$ and A^{-1} for $\{x^{-1} : x \in A\}$. Also, if $a \in G$, we write aB and Ba respectively for $\{a\}B$ and $B\{a\}$ and call them the **left and right translate** of B by a. Finally, we shall sometimes write A^n for $A \ldots A$ (n times).

A set $\mathcal{F}$ of subsets of a set E is a **filter** on E if $E \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$, the intersection of any two members of $\mathcal{F}$ again belongs to $\mathcal{F}$, and any subset of E containing a member of $\mathcal{F}$ also belongs to $\mathcal{F}$. In a topological space E a **neighbourhood** of a point c is any subset of E containing an open set U such that $c \in U$; the set of all neighbourhoods of c is thus a filter on E. Similarly, a **neighbourhood of a subset** C of E is any subset of E containing an open set U such that $C \subset U$, and the set of all neighbourhoods of C is also a filter on E. A set $\mathcal{B}$ of subsets of E is a **filter base** on E if the set of all subsets F of E for which there exists $B \in \mathcal{B}$ such that $B \subset F$ is a filter, called the **filter generated** by $\mathcal{B}$. Thus, $\mathcal{B}$ is a filter base iff $\mathcal{B} \neq \emptyset$, $\emptyset \notin \mathcal{B}$, and the intersection of two members of $\mathcal{B}$ contains a member of $\mathcal{B}$. Consequently, a filter base on E is also a filter base on any set containing E. In a topological space E, a **fundamental system of neighbourhoods** of $c \in E$ is any filter base generating the filter of neighbourhoods of c; i.e. a fundamental system of neighbourhoods of $c \in E$ is a set $\mathcal{F}$ of neighbourhoods of c such that every neighbourhood of c contains a member of $\mathcal{F}$.

Let G be a topological group, and let $\mathcal{V}$ be the filter of neighbourhoods of 1. Since the left and right translations by an element $a \in G$ are homeomorphisms, then (cf. the basic principle above) $a\mathcal{V}$ and $\mathcal{V}a$ are both the filter of neighbourhoods of a (where $a\mathcal{V} := \{aV : V \in \mathcal{V}\}$ and $\mathcal{V}a = \{Va : V \in \mathcal{V}\}$). Since $(x, y) \longrightarrow xy$ is continuous at $(1, 1)$ and since the functions $j : x \mapsto x^{-1}$ and $T_a : x \mapsto axa^{-1}$, both from $G \longrightarrow G$, are homeomorphisms, $\mathcal{V}$ has the following properties:

TGN 1 For each $V \in \mathcal{V}$ there exists $U \in \mathcal{V}$ such that $UU \subset V$.

TGN 2 If $V \in \mathcal{V}$, then $V^{-1} \in \mathcal{V}$.

TGN 3 If $V \in \mathcal{V}$, then for each $a \in G$, $aVa^{-1} \in \mathcal{V}$.

These properties characterize the filter of neighbourhoods of 1 in a topological group in the following sense:

Theorem II.4.2 *Let G be a group. If $\mathcal{V}$ is a filter on G satisfying (TGN 1), (TGN 2) and (TGN 3), then there is a unique group topology on G for which $\mathcal{V}$ is the filter of neighbourhoods of* 1.

Proof. If τ is such a topology, then, since a set is open iff it is a neighbourhood of each of its points, and since l_a is a homeomorphism for each $a \in G$, a subset O of G is open for τ iff

$(*)$ for each $a \in O$ there exists $V \in \mathcal{V}$ such that $aV \subset O$.

Thus, there is at most one group topology on G for which $\mathcal{V}$ is the filter of neighbourhoods of 1.

It remains to show that the set τ of all the sets O satisfying $(*)$ is a group topology for which $\mathcal{V}$ is the filter of neighbourhoods of 1. Clearly, $G \in \tau$, $\emptyset \in \tau$, and the union of a family of members of τ belongs to τ. Let O_1, $O_2 \in \tau$; if $a \in O_1 \cap O_2$, there exist V_1, $V_2 \in \mathcal{V}$ such that $aV_1 \subset O_1$ and $aV_2 \subset O_2$, so $V_1 \cap V_2 \in \mathcal{V}$ and $a(V_1 \cap V_2) = aV_1 \cap aV_2 \subset O_1 \cap O_2$. Thus, τ is a topology on G.

To show that $\mathcal{V}$ is the filter of neighbourhoods of 1 for τ, let $V \in \mathcal{V}$. We shall first show that $1 \in V$. By (TGN 1) there exists $U \in \mathcal{V}$ such that $UU \subset V$, and by (TGN 2), $U^{-1} \in \mathcal{V}$; hence $U \cap U^{-1} \in \mathcal{V}$, so there exists $x \in U \cap U^{-1}$. Then both x and x^{-1} belong to U, so $1 = xx^{-1} \in UU \subset V$. To show that V is a neighbourhood of 1, let $O = \{a \in G :$ there exists $U \in \mathcal{V}$ such that $aU \subset V\}$. As $1V = V$, $1 \in O$, and as each $U \in \mathcal{V}$ contains 1, $O \subset V$. Therefore we need only show that $O \in \tau$. Let $a \in O$. Then there exists $U \in \mathcal{V}$ such that $aU \subset V$. By (TGN 1) there exists $W \in \mathcal{V}$ such that $WW \subset U$. Then $aW \subset O$, for if

$w \in W$, $awW \subset aWW \subset aU \subset V$, so $aw \in O$. Therefore $O \in \tau$ since O satisfies $(*)$. Conversely, if V is a neighbourhood of 1, there exists $O \in \tau$ such that $1 \in 0 \subset V$, so by (*), there exists $U \in \mathcal{V}$ such that $U = 1U \subset O \subset V$, whence $V \in \mathcal{V}$.

Finally, we need to verify that if $a, b \in G$, then $(x, y) \mapsto xy^{-1}$ is continuous at (a, b), that is, for each $U \in \mathcal{V}$ there exists $V \in \mathcal{V}$ such that if $x \in aV$ and $y \in bB$, then $xy^{-1} \in ab^{-1}U$. By (TGN 3), $b^{-1}Ub \in \mathcal{V}$, and by (TGN 1) there exists $W \in \mathcal{V}$ such that $WW \subset b^{-1}Ub$. Let $V := W \cap W^{-1}$. By (TGN 2), $V \in \mathcal{V}$. Let $x \in aV$ and $y \in bV$. Then, $x = av$ and $y = bw$ where $v, w \in V$. Hence $w^{-1} \in V \subset W$, so

$$xy^{-1} = avw^{-1}b^{-1} \in aWWb^{-1} \subset a(b^{-1}Ub)b^{-1} = ab^{-1}U. \blacksquare$$

Corollary II.4.3 *Let G be a group. If $\mathcal{B}$ is a fundamental system of neighbourhoods of 1 for a group topology on G, then the following conditions hold:*

TGB 1 *For each $V \in \mathcal{B}$ there exists $U \in \mathcal{B}$ such that $UU \subset V$.*

TGB 2 *If $V \in \mathcal{B}$, then there exists $U \in \mathcal{B}$ such that $U \subset V^{-1}$.*

TGB 3 *If $V \in \mathcal{B}$, then for each $a \in G$ there exists $U \in \mathcal{B}$ such that $U \subset aVa^{-1}$.*

Conversely, if $\mathcal{B}$ is a filter base on G satisfying (TGB 1), (TGB 2) and (TGB 3), then there is a unique group topology on G for which $\mathcal{B}$ is a fundamental system of neighbourhoods of 1. $\blacksquare$

Thus, to define a group topology on a group G, it suffices to specify a filter base $\mathcal{B}$ satisfying (TGB 1), (TGB 2) and (TGB 3) as a fundamental system of neighbourhoods of 1. Thus any collection of subgroups of G containing all conjugates of its members and all finite intersections of its members (in particular any chain of normal subgroups of G), defines a topological group structure on G. For example, if $\mathcal{B}$ is a filter base of normal subgroups of G, then $\mathcal{B}$ is a fundamental system of neighbourhoods of 1 for a group topology on G.

A subset A of a group G, denoted multiplicatively (additively) is **symmetric** if $A^{-1} = A$ ($-A = A$).

Theorem II.4.4 *Let G be a topological group, let $\mathcal{V}$ be a fundamental system of neighbourhoods of 1, and let $A \subset G$.*

(1) If O is an open subset of G, then AO and OA are open; hence for any neighbourhood V of 1, AV and VA are neighbourhoods of A.

(2) The symmetric open neighbourhoods of 1 form a fundamental system of neighbourhoods of 1.

(3) $\overline{A} = \bigcap\{AV : V \in \mathcal{V}\} = \bigcap\{VA : V \in \mathcal{V}\}$; in particular, $\overline{\{1\}} = \bigcap\{V : V \in \mathcal{V}\}$.

(4) The closed symmetric neighbourhoods of 1 form a fundamental system of neighbourhoods of 1.

Proof. (1) For each $a \in A$, aO and Oa are open, since left and right multiplication by a are homeomorphisms. So as $AO = \bigcup\{aO : a \in A\}$ and $OA = \bigcup\{Oa : a \in A\}$, AO and OA are also open.

(2) If O is an open neighbourhood of 1, then so is O^{-1}, since $g \mapsto g^{-1}$ (where $g \in G$) is a homeomorphism, so $O \cap O^{-1}$ is a symmetric open neighbourhood of 1 contained in O.

(3) Let $b \in \overline{A}$, and let $V \in \mathcal{V}$. By (TGN 2), bV^{-1} and $V^{-1}b$ are neighbourhoods of b, so there exist $x \in bV^{-1} \cap A$ and $y \in V^{-1}b \cap A$. Thus, $b \in xV \subset AV$ and $b \in Vy \subset VA$. Conversely, let $b \in \bigcap\{AV : V \in \mathcal{V}\}$. Then for any $U \in \mathcal{V}$, there exists $V \in \mathcal{V}$ such that $V \subset U^{-1}$, so as $b = av$ for some $a \in A$, $v \in V$, $a = bv^{-1} \in bU$. Thus every neighbourhood of b intersects A non–vacuously, so $b \in \overline{A}$. Similarly, $\bigcap\{VA : V \in \mathcal{V}\} = \overline{A}$.

(4) If U is a neighbourhood of 1, there exists a neighbourhood V of 1 such that $VV \subset U$, and by (3), $\overline{V} \subset VV \subset U$. Thus every neighbourhood of 1

contains a closed neighbourhood of 1. If U is a closed neighbourhood of 1, so is U^{-1}, so $U \cap U^{-1}$ is a closed symmetric neighbourhood of 1 contained in U. ∎

A topological space E is **regular** if E is Hausdorff and for each $b \in E$ the closed neighbourhoods of b form a fundamental system of neighbourhoods of b (i.e. given any neighbourhood of a point of E there's always a closed neighbourhood contained in it). In this case, we also call the topology of E a **regular topology**.

We shall now introduce uniformity concepts that arise naturally from the topology of a topological group.

Let E be a topological space, $\mathcal{B}$ a filter base on E. The filter base $\mathcal{B}$ **converges** to $c \in E$ if the filter generated by $\mathcal{B}$ converges to c, that is, if every neighbourhood of c contains a member of $\mathcal{B}$. If E is Hausdorff, $\mathcal{B}$ converges to at most one point of E, for if U and V are disjoint neighbourhoods of two points of E, the filter generated by $\mathcal{B}$ can not contain both U and V since then it would contain the empty set $U \cap V$.

Let G be a topological group, denoted multiplicatively. If V is a neighbourhood of 1, a subset F of G is **V–small** if $F^{-1}F \subset V$ and $FF^{-1} \subset V$. A filter (base) on G is a **Cauchy filter (base)** if for every neighbourhood V of 1 it contains a V–small set. A subset E of a topological group G is **complete** if every Cauchy filter on E converges to a point of E.

In the proof of Cohn's embedding we shall need to extend a certain mapping θ from a dense subset of a topological space to the whole topological space, so we require the following

Theorem II.4.5 (Extension by continuity) *Let X be a topological space, A a dense subset of X, $\theta: A \longrightarrow Y$ a mapping of A into a regular space Y. A sufficient condition for θ to extend[3] to a continuous mapping $\bar{\theta}: X \longrightarrow Y$ is that,*

[3] *Actually, this condition is also necessary and the extension is unique, but we shall not need these facts, see Bourbaki [Bou74], Ch. I.*

for each $x \in X$, $\theta(y)$ tends to a limit in Y when y tends to x while remaining in A.

Proof. Define $\bar{\theta}(x) = \lim_{y \to x, y \in A} \theta(y)$ for each $x \in X$; $\bar{\theta}(x)$ is a well–defined element of Y, since Y is Hausdorff. We have to show that $\bar{\theta}$ is continuous at each point $x \in X$. Let then V' be a closed neighbourhood of $\bar{\theta}(x)$ in Y; then by hypothesis there is an open neighbourhood V of x in X such that $\theta(V \cap A) \subset V'$. Since V is a neighbourhood of each of its points, we have

$$\bar{\theta}(z) = \lim_{y \to x, y \in V \cap A} \theta(y)$$

for each $z \in V$, and from this it follows that $\bar{\theta}(z) \in \overline{\theta(V \cap A)} \subset V'$, since V' is closed. The result now follows from the fact that the closed neighbourhoods of $\theta(x)$ form a fundamental system of neighbourhoods of $\theta(x)$ in Y, since Y is regular. ∎

The mapping $\bar{\theta}$ is said to be obtained by **extending θ by continuity** to X.

In section II.6 we shall need the fact that certain group topology be regular in order to be able to extend certain mapping by continuity. This will be achieved by checking condition (2) of the following

Theorem II.4.6 *Let G be a topological group. The following statements are equivalent:*

(1) $\{1\}$ *is closed.*

(2) $\{1\}$ *is the intersection of all neighbourhoods of* 1.

(3) G is Hausdorff.

(4) G is regular[4].

[4] *Note that, following Bourbaki, we asked the Hausdorff property for a space to be regular, some authors don't ask this extra condition, and then, for them every topological group is regular.*

Proof. (1) and (2) are equivalent by (3) of theorem II.4.4, and (3) and (4) are equivalent by (4) of theorem II.4.4. Clearly (3) only if (1). To finish the proof of the theorem is enough to show that (2) only if (3). Assume (2), and let a and b be distinct points of G. Then $1 \neq a^{-1}b$, so there is a neighbourhood U of 1 such that $a^{-1}b \notin U$. Let V be a symmetric neighbourhood of 1 such that $VV \subset U$. Then aV and bV are disjoint neighbourhoods of a and b respectively, for if $av = bw$ where $v, w \in W$, then $a^{-1}b = vw^{-1} \in VV \subset U$, a contradiction. ∎

Finally, as the last background material to prove Cohn's embedding theorem (see section II.6, page 91) we need a definition of fields which uses as little as possible of the additive properties. This will be accomplished in the following well known technical result which will be quoted without proof (cf. Cohn [Coh61], Dauns [Dau70], Dicker [Dic68], and Rabinow [Rab37]), where we shall describe a set of axioms for skew fields in terms of multiplication and the operation $x \mapsto 1 - x$.

Lemma II.4.7 *Let G be a multiplicative group and G_1 the subset $G_1 := \{x \in G : x \neq 1\}$. Also, let $\{0\}$ be any singleton disjoint with G. A necessary and sufficient condition for addition to be definable on $G \cup \{0\}$ so that $G \cup \{0\}$ becomes a skew field with the original group operation of G as multiplication, supplemented with $0x = 0 = x0$ $(x \in G)$, and 0 as the neutral element for this addition is that there exists an element $e \in G$ and a function $\theta : G_1 \longrightarrow G$ which for any $x, y \in G_1$ satisfy the following:*

$$(i) \qquad \theta(yxy^{-1}) = y\theta(x)y^{-1}$$

$$(ii) \qquad \theta^2(x) = x$$

$$(iii) \qquad \theta(x^{-1}) = e\theta(x)x^{-1}$$

$$(iv) \qquad \theta(xy^{-1}) = \theta(\theta(x)\theta(y)^{-1}).\theta(y^{-1}), \quad x \neq y.$$

If there do exist such an e and θ, then

$$\theta(x) = 1 - x \tag{II.9}$$

$$e = -1. \tag{II.10}$$ ∎

Essentially, what the above lemma says is that given any multiplicative group $(G, .)$ and an extra element 0 (not in G), as soon as you have a mapping θ from $G_1 := G - \{1\}$ to G and an element $e \in G$ satisfying conditions (i)–(iv), you can define an addition $+$ on $G \cup \{0\}$ so that $(G \cup \{0\}, +, .)$ becomes a skew field. If this is the case, we have the additional information that θ turns out to be the mapping $x \mapsto 1 - x$ and $e = -1$. In the proof of Cohn's embedding, G will be an inverse limit of certain groups (to be constructed with an embedding theorem for semigroups, section II.5) and 0 will be the zero element of a suitable ring R to be embedded in a skew field. We shall be able to find an element $e \in G$ and a function θ satisfying the conditions of the above lemma, so $G \cup \{0\}$ will become a skew field. It will turn out that R^*, the multiplicative semigroup of R will be embedded in G and the additive group of R will be a subgroup of the additive group of $G \cup \{0\}$.

II.5 An embedding theorem for a class of inverse limit semigroups

The proof of Cohn's embedding theorem (see section II.6, page 91) will proceed by embedding R^*, the multiplicative semigroup of a "suitable" ring R, in a group constructed as an inverse limit. So, in this section, we shall prove an embedding theorem for semigroups.

We begin with a semigroup S (come again, which in the application we have in mind will be the multiplicative semigroup of a ring). Recall that a **congruence relation** in S is an equivalence relation such that $a \equiv a'$ and

$b \equiv b'$ only if $ab \equiv a'b'$. If $\overline{S}$ is the quotient set determined by $\equiv$ then $\overline{S}$ is a semigroup relative to the composition $\overline{a}\overline{b} = \overline{ab}$, where $\overline{a}$ denotes the equivalence class of the element $a \in S$. We call $\overline{S}$ the **quotient semigroup** determined by $\equiv$ in S.

Suppose that for each $n \in \mathbb{N}$ we have a group G_n and that for each pair $n \leq m$ we have a group homomorphism $\phi_n^m : G_m \longrightarrow G_n$ satisfying the **coherence conditions**:

(i) each $\phi_m^m : G_m \longrightarrow G_m$ is the identity,

(ii) if $l \leq n \leq m$ then $\phi_l^n \circ \phi_n^m = \phi_l^m$.

We then call $\{G_m, \phi_n^m\}_{m \leq n,\, m,\, n \in \mathbb{N}}$ a **projective or inverse system** of groups directed by $\mathbb{N}$. The subgroup[5]

$$G := \left\{ x = (x_n)_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} G_n : \phi_n^m(x_m) = x_n, \text{ for all } n \leq m \text{ in } \mathbb{N} \right\}$$

of the product[6] $\prod_{n \in \mathbb{N}} G_n$ is called the **projective or inverse limit** of the inverse system $\{G_m, \phi_n^m\}_{m \leq n,\, m,\, n \in \mathbb{N}}$.

Theorem II.5.1 *Let S be a multiplicative semigroup. For each $n \in \mathbb{N}$ let $\equiv_n$ be a congruence relation in S. Assume that the following conditions hold:*

(i) *if $m \geq n$ $(m, n \in \mathbb{N})$ then, $a \equiv_m b$ $(a, b \in S)$ only if $a \equiv_n b$;*

(ii) *if $a \equiv_n b$ for all $n \in \mathbb{N}$ then $a = b$;*

(iii) *for each $n \in \mathbb{N}$ the quotient semigroup $S_n := (S/\equiv_n)$ determined by $\equiv_n$ in S satisfies the cancellation laws and has the right common multiple property.*

---

[5] For a complete introduction to limits in any category cf., for instance, Eilenberg and Steenrod [ES52], Herrlich and Strecker [HS73] or Mac Lane [ML71]; one sees that in the category of groups inverse limits always exist, i.e. G is indeed a group which has a certain universal property.

[6] Product in the category of groups.

Then S may be embedded in a group G; moreover, there is a group topology defined on G, which is regular, such that G becomes a complete topological group and SS^{-1} is dense in G.

Proof. Let $a \in S$. The first condition shows that if $[a]_m$ denotes the equivalence class of a relative to $\equiv_m$ and $m \geq n$ then $[a]_m \mapsto [a]_n$ is a semigroup homomorphism ϕ_n^m from S_m into S_n. By corollary I.2.8 (page 18), the third condition shows that S_m can be embedded in a group G_m of right quotients, i.e. $G_m = S_m S_m^{-1}$ and that ϕ_n^m can be extended to a unique homomorphism of G_m to G_n, which we denote again by ϕ_n^m. By direct verification we see that each $\phi_m^m : G_m \longrightarrow G_m$ is the identity, and if $l \leq n \leq m$ then $\phi_l^n \circ \phi_n^m = \phi_l^m$. Since the coherence conditions hold, we can form the inverse limit group $G := \{x = (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} G_n : \phi_n^m(x_m) = x_n, \text{ for all } n \leq m \text{ in } \mathbb{N}\}$ of the inverse system $\{G_m, \phi_n^m\}_{m\leq n,\, m,n\in\mathbb{N}}$. We have the canonical homomorphism $\theta_m : a \mapsto [a]_m$ of S onto S_m which can be considered as a homomorphism of S into G_m (since S_m is embedded in G_m). Let $m, n \in \mathbb{N}$, by definition of ϕ_n^m and θ_m we also have that

$$(*) \qquad \phi_n^m \circ \theta_m = \theta_n, \text{ if } m \geq n.$$

This shows that we have a homomorphism θ of S into G such that for all $m \in \mathbb{N}$, $\pi_m \circ \theta = \theta_m$, where π_m is the projection of the inverse limit G onto G_m. It follows from condition (ii) that θ is an embedding of S into the group G. Thus, any semigroup satisfying conditions (i)–(iii) can be embedded in a group.

Note that the kernels $\{ker\, \pi_m\}_{m\in\mathbb{N}}$ form a filter base of normal subgroups of G, i.e. $\{ker\, \pi_m\}_{m\in\mathbb{N}}$ is non–empty, $\emptyset \notin \{ker\, \pi_m\}_{m\in\mathbb{N}}$, and the intersection of two members of it contains a member of it (actually, if $m \geq n$ then $ker\, \pi_m \subset ker\, \pi_n$, by condition $(*)$ and since every group homomorphism sends 1 to 1). Hence, by corollary II.4.3 (page 82, see also the paragraph following it), G becomes a topological group if the normal subgroups $K_m := ker\, \pi_m$ $(m \in \mathbb{N})$

are taken as a neighbourhood base at 1. Being G the inverse limit of the family $\{G_m, \phi_n^m\}_{m \leq n, m, n \in \mathbb{N}}$, G is complete in the topology thus defined.

Also, since

$$\bigcap_{m \in \mathbb{N}} ker\, \pi_m = \{1\}$$

then it follows that condition (2) of theorem II.4.6 (page 85) holds, i.e. $\{1\}$ is the intersection of all neighbourhoods of 1, hence this topology is regular.

Finally, we show that SS^{-1} is dense in G. Let $x = (x_m)_{m \in \mathbb{N}} \in G$. Since $G_m = S_m S_m^{-1}$ then $x_m = [a]_m [b]_m^{-1}$, for some $a, b \in S$. Note that $G/K_m \cong G_m$, so $xK_m = ab^{-1}K_m$, that is $x \equiv ab^{-1} \,(mod\, K_m)$. Therefore, SS^{-1} is dense in G. ∎

Remark II.5.2 *Let $\equiv_m$ and K_m be as in the proof of theorem II.5.1. Note that for all $a\, b \in S$,*

$$a \equiv_m b \text{ iff } a \equiv b \,(mod\, K_m).$$ ∎

It follows that for all $a, b, c, d \in S$

$$ab^{-1} \equiv cd^{-1} \,(mod\, K_m) \text{ iff}$$

$$\text{there exist } x, y \in S \text{ such that } ax \equiv_m cy \text{ and } bx \equiv_m dy,$$

indeed, if $ab^{-1} \equiv cd^{-1} \,(mod\, K_m)$ then $ab^{-1}K_m = cd^{-1}K_m$ in G/K_m. So, $aK_m = c(d^{-1}b)K_m$. But since $G/K_m \cong G_m$ and $G_m = S_m S_m^{-1}$ we have $[d]_m^{-1}[b]_m = [y]_m[x]_m^{-1}$ for some $y, x \in S$. Hence, $aK_m = cyx^{-1}K_m \longrightarrow axK_m = cyK_m \longrightarrow ax \equiv_m cy$. Also, since $b^{-1}dK_m = a^{-1}cK_m$ we have $axK_m = cyK_m \longrightarrow xy^{-1}K_m = a^{-1}cK_m \longrightarrow xy^{-1}K_m = b^{-1}dK_m \longrightarrow bxK_m = dyK_m$, hence $bx \equiv_m dy$.

Conversely, if there exist $x, y \in S$ such that $ax \equiv_m cy$ and $bx \equiv_m dy$, then we obtain $a^{-1}cK_m = xy^{-1}K_m = b^{-1}dK_m$, hence $b^{-1}dK_m = a^{-1}cK_m$, and then $ab^{-1}K_m = cd^{-1}K_m$. ∎

II.6 Cohn's embedding theorem

Suppose that the multiplicative semigroup $R^\bullet$ of a non–commutative integral domain R can be embedded in a group G. Bokut [Bok69], Bowtell [Bow67] and Klein [Kle67] gave examples of rings R for which an embedding $R^\bullet \hookrightarrow G$ is possible, but such that for any embedding of $R^\bullet$ into any group G whatever, addition cannot be extended to all of $G \cup \{0\}$ in order to obtain an embedding of R into a division ring, answering in the negative a question raised by Malcev [Mal37] who asked if a ring R such that $R^\bullet$ is embeddable in a group must be embeddable in a field.

In this section we shall see that under certain appropriate additional hypotheses on an integral domain R with a valuation into the integers, Cohn [Coh61] embeds $R^\bullet \hookrightarrow G \cup \{0\}$, where $(G, .)$ is a certain inverse limit group, introduces a group topology on G, then defines an addition $+$ on the subset $R^\bullet R^{\bullet -1}$ which happens to be dense in G, and then finally extends addition to all of G, so that $(G, +, .)$ becomes a skew–field and R a subring of it.

A ring R is said to be **valuated**[7] if a function $v(x)$ is defined on R taking the integers or $+\infty$ as values, such that

V.1 $v(x) = \infty$ iff $x = 0$,

V.2 $v(xy) = v(x) + v(y)$,

V.3 $v(x - y) \geq min\{v(x), v(y)\}$.

The function v is also called a **valuation** on R. From V.1 and V.2 it follows that R has no zero–divisors (we don't consider 0 a zero divisor), so that $R^\bullet$ is a cancellation semigroup, and from V.3 one deduces[8] as in the case of valuations

[7] For a survey in valuation theory, cf. Schilling [Sch50] or, Zariski and Samuel [ZS60].
[8] See footnote 7 on page 91.

on fields that

(II.11) $$v(-x) = v(x),$$

and

(II.12) $$v(x \pm y) = min\{v(x), v(y)\} \text{ unless } v(x) = v(y).$$

With these definitions we are ready to state

Theorem II.6.1 (Cohn's embedding theorem) *Let R be a valuated ring such that for any $a, b \in R^*$ the function $f: R^* \times R^* \longrightarrow \mathbb{Z} \cup \{+\infty\}$, defined by*

$$f(x, y) := v(ax - by) - v(ax)$$

is unbounded above. Then R can be embedded in a skew field.

Before giving the proof, let's discuss the essential details of the argument. So, let R be a ring with a valuation v satisfying the condition in the theorem. Being R valuated, it is an integral domain, so the set R^* of non–zero elements is a semigroup relative to the multiplication defined in R. For each $n \in \mathbb{N}$ we shall define a congruence relation $\equiv_n$ in R^* by the rule $a \equiv_n b$ iff $v(a-b) - v(a) \geq n$. We shall show that the set of congruences $\{\equiv_n\}_{n \in N}$ satisfy conditions (i)–(iii) of the semigroup embedding theorem II.5.1 (page 88) and then it will follow that R^* can be embedded in the manner indicated in that theorem in a group G.

It will remain to define an addition in $K := G \cup \{0\}$ (where 0 is the zero element of R) so that K with this addition and the multiplication in K, which is the multiplication in G supplemented by $0x = 0 = x0$ ($x \in K$), is a division ring containing R as a subring. To achieve this we shall define a mapping θ in $G_1 := \{x \in G : x \neq 1\}$ and an element $e \in G$ which in the end turn out

to be the mapping $x \mapsto 1 - x$ and $e = -1$. The connection between addition, and the mapping θ and e is given by the characterization of skew fields given in lemma II.4.7 (page 86).

In order to define θ and e for the group G constructed from R^* we shall proceed as follows. We let $U_1 = \{ab^{-1} : a, b \in R^*, a \neq b\}$ and define a mapping θ from U_1 to G_1 by $\theta(ab^{-1}) = (b-a)b^{-1}$. Of course, we shall have to check that this mapping is single value. Next, we shall show that if a and b are any two elements in R^* then $(-a)a^{-1} = (-b)b^{-1}$. We shall take this element $(-a)a^{-1}$ which is independent of a to be the element e. We shall see that this mapping θ can be extended (using continuity and the density of U_1 in G_1) to a mapping θ in G_1, which together with e, will satisfy condition (i)–(iv) of lemma II.4.7 (page 86). This will give us a division ring structure in K such that R is a subring of K and the theorem will be proved.

Now we are ready to present the

Proof of Cohn's embedding theorem II.6.1. Since R is a valuated ring, it must be an integral domain, as we already observed. In order to be able to apply the semigroup embedding theorem II.5.1 (p. 88) we define, for each $n \in \mathbb{N}$, a relation $\equiv_n$ in R^* by putting

$$a \equiv_n b \text{ iff } v(a-b) - v(a) \geq n. \tag{II.13}$$

If $a \equiv_n b$, $n \in \mathbb{N}$ then $v(a-b) > v(a)$ and hence, by (II.12),

$$v(b) = v(a - (a-b)) = v(a),$$

i.e.

$$a \equiv_n b \ (n \in \mathbb{N}) \text{ only if } v(a) = v(b). \tag{II.14}$$

It is clear that the relation $\equiv_n$ is reflexive and by (II.14) it is also symmetric. We

now show transitivity. Assume $a \equiv_n b, b \equiv_n c$, then by (II.14) $v(a) = v(b) = v(c)$ and

$$v(a-c) \geq min\{v(a-b), v(b-c)\} \geq n + v(a),$$

whence $a \equiv_n c$. So, each $\equiv_n$ is an equivalence relation in R^*.

We now show that $\equiv_n$ is a congruence in R^* and that conditions (i)–(iii) of theorem II.5.1 hold. Of these (i) follows immediately from the definitions. To prove (ii), let $a \neq b$, then $v(a-b) \neq \infty$; hence we can choose $k \in \mathbb{N}$ so that $k > v(a-b) - v(a)$ and for this k, $a \not\equiv_n b$, so (ii) holds. We now show (iii), we take $a, b \in R^*$; then

$$v(a) = v(b) \text{ iff } v(ac) = v(bc) \text{ iff } v(ca) = v(cb);$$

further we have

$$\begin{aligned} v(ac-bc) - v(ac) &= v((a-b)c) - v(ac) \\ &= v(a-b) + v(c) - v(c) - v(a) \\ &= v(a-b) - v(a), \end{aligned}$$

and similarly $v(ca-cb) - v(ca) = v(a-b) - v(a)$. It follows that

$$a \equiv_n b \text{ iff } ac \equiv_n bc \text{ iff } ca \equiv_n cb,$$

and this shows that $R^*/\equiv_n$ is a cancellation semigroup. We now check the right multiple condition for $R^*/\equiv_n$: given $a, b \in R^*$ and $n \in \mathbb{N}$, there exist $x, y \in R^*$ such that

$$v(ax-by) - v(ax) \geq n$$

and hence $ax \equiv_n by$. So, (iii) holds.

Since all the hypotheses of theorem II.5.1 are satisfied, R^* may be embedded in a regular complete topological group G such that R^*R^{*-1} is dense in G.

As in the proof of theorem II.5.1, let $K_n := ker\,\pi_n$, where $\pi_n : G \longrightarrow G_n$ is the projection onto the n–th factor G_n the group of right quotients of $R^\bullet / \equiv_n$. By remark II.5.2 (p. 90),

$$ab^{-1} \equiv cd^{-1}\,(mod\,K_n) \tag{II.15}$$

holds iff there exist $x, y \in R^\bullet$ such that

$$ax \equiv_n cy, \qquad bx \equiv_n dy. \tag{II.16}$$

If this condition is satisfied, then $v(a) - v(b) = v(c) - v(d)$, so that the valuation may be extended to $R^\bullet R^{\bullet -1}$ by putting

$$v(ab^{-1}) = v(a) - v(b). \tag{II.17}$$

By (II.14), (II.15), (II.16), v is constant on the cosets of K_n in G, for every $n \in \mathbb{N}$, and it may therefore be extended in a natural way to a function defined on the whole of G and taking integers values. Like v, this function is again a homomorphism (into the additive group of the integers) and we may, without ambiguity, denote this function on G again by v.

Write

$$G_1 := \{x \in G : x \neq 1\}, \qquad U_1 := \{ab^{-1} \in R^\bullet R^{\bullet -1}\};$$

note that since $R^\bullet R^{\bullet -1}$ is dense in G, then U_1 is dense in G_1. Now we define a mapping θ from U_1 to G_1 by

$$\theta(ab^{-1}) = (b - a)b^{-1}. \tag{II.18}$$

Of course we have to show that θ is single–value: if

$$ab^{-1} = cd^{-1} \quad (a, b, c, d \in R^*),$$

then $b^{-1}d = a^{-1}c$ and there exist $x_n y_n^{-1} \in R^* R^{*-1}$ such that $x_n y_n^{-1} \longrightarrow b^{-1}d$.

Thus $v(bx_n - dy_n) - v(bx_n) \longrightarrow \infty$; this may be written

$$v((bx_n - dy_n)x_n^{-1}) - v(b) \longrightarrow \infty,$$

or since $v(b)$ is constant,

$$v((bx_n - dy_n)x_n^{-1}) \longrightarrow \infty. \tag{II.19}$$

Similarly, since $x_n y_n^{-1} \longrightarrow b^{-1}d = a^{-1}c$, we have

$$v((ax_n - cy_n)x_n^{-1}) \longrightarrow \infty. \tag{II.20}$$

By (II.19) and (II.20), $v([(b-a)x_n - (d-c)y_n]x_n^{-1}) \longrightarrow \infty$, whence $(b-a)x_n y_n^{-1} \longrightarrow d - c$. Multiplying both sides by d^{-1} and observing that $x_n y_n^{-1} \longrightarrow b^{-1}$, we obtain

$$(b-a)b^{-1} = \lim_{n \longrightarrow \infty} (b-a)x_n y_n^{-1} d^{-1} = (d-c)d^{-1}.$$

This shows θ to be single–value on U_1. In order to extend θ by continuity to G_1 we require the following lemma.

Lemma II.6.2 *If $u \in G_1$ and $(u_n)_{n \in \mathbb{N}}$ is any sequence of elements of U_1 converging to u, then $\lim_{n \longrightarrow \infty} \theta(u_n)$ exists.*

Proof of lemma II.6.2. To establish the convergence of $(\theta(u_n))_{n \in \mathbb{N}}$ it is enough to show that $(\theta(u_n))_{n \in \mathbb{N}}$ is a Cauchy sequence; writting

$$u_n := a_n b_n^{-1} \, (a_n, b_n^{-1} \in R^*),$$

we have to show that for any $r \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ such that

(II.21) $\quad (b_m - a_m)b_m^{-1} \equiv (b_n - a_n)b_n^{-1} \pmod{K_r} \quad$ for $m, n > n_0$.

Since $a_n b_n^{-1} \longrightarrow u$, we have

(II.22) $\quad v(a_n b_n^{-1}) = v(u) =: h$ say, for $n > n_1$.

On the other hand, $u \neq 1$ and so there exist $k, n_2 \in \mathbb{N}$ such that $a_n b_n^{-1} \not\equiv 1 \pmod{K_k}$ for $n > n_2$, i.e. $a_n \not\equiv b_n \pmod{K_k}$, whence

(II.23) $\quad v((b_n - a_n)a_n^{-1}) < k$ for $n > n_2$.

Now take a fixed r, put $s := max\{r + k, r + k + h\}$ and choose n_3 so that

(II.24) $\quad a_m b_m^{-1} \equiv a_n b_n^{-1} \pmod{K_s}$ for $m, n > n_3$.

We assert that (II.21) holds for $n_0 := max\{n_1, n_2, n_3\}$. For, by (II.24), there exist $x, y \in R^*$ such that

(II.25) $\quad a_m x \equiv a_n y \pmod{K_s}$,

(II.26) $\quad b_m x \equiv b_n y \pmod{K_s}$,.

These congruences may be written

(II.27) $\quad v((a_m x - a_n y)(a_m x)^{-1} \geq s$,

(II.28) $\quad v((b_m x - b_n y)(b_m x)^{-1} \geq s$.

By (II.22), $v(b_m a_m^{-1}) = -h$, so that (II.28) may be written as

(II.29) $\quad v((b_m x - b_n y)(a_m x)^{-1} \geq s - h$.

Using (II.27), (II.29),and (II.23) we now find

$$
\begin{aligned}
&v([(b_m - a_m)x - (b_n - a_n)y][(b_m - a_m)x]^{-1}) \\
&= v(b_m x - a_m x - b_n y + a_n y) - v((b_m - a_m)x) \\
&= v((a_m x - a_n y)(a_m x)^{-1} - (b_m x - b_n y)(a_m x)^{-1}) + v(a_m x) - v((b_m - a_m)x) \\
&\geq min\{v((a_m x - a_n y)(a_m x)^{-1}), v((b_m x - b_n y)(a_m x)^{-1})\} - v((b_m - a_m)a_m^{-1}) \\
&\geq min\{s,\ s - h\} - k = r;
\end{aligned}
$$

hence

$$(b_m - a_m)x \equiv (b_n - a_n)y\,(mod\,K_r). \tag{II.30}$$

Now $k > 0$; hence $s \geq r + k > r$ and so we deduce from (II.26)

$$b_m x \equiv b_n y\,(mod\,K_r). \tag{II.31}$$

The congruences (II.30) and (II.31) hold for any $m\,n \geq n_0$; taken together they provide (II.21) and the proof of the lemma is completed.

Thus θ is a mapping from a dense subset U_1 of G_1 into G_1 such that $\lim_{n\longrightarrow\infty} \theta(u_n)$ exists whenever $u_n \longrightarrow u$. Since G is regular, then by theorem II.4.5 (p. 84) we may extend θ to a continuous mapping of G_1 into itself; such an extension will be denoted again by θ.

Now, we shall define an element $e \in G$. Let $a \in R^*$ and consider the element $(-a)a^{-1}$ of G. If b is any other element of R^* and $n \in \mathbb{N}$, then there exist $x, y \in R^*$ such that

$$v(ax - by) - v(ax) \geq n; \tag{II.32}$$

hence

$$v((-a)x-(-b)y)-v((-a)x)\geq n \tag{II.33}$$

and we conclude that

$$(-a)a^{-1}\equiv(-b)b^{-1}\,(mod K_n),\ \text{for all } n\in\mathbb{N}, \tag{II.34}$$

in other words,

$$(-a)a^{-1}=(-b)b^{-1}=:e,\ \text{say.}$$

We complete the proof of the theorem by showing that G satisfies the conditions of lemma II.4.7 (page 86), with the θ and e just defined.

(i) If $ab^{-1}\in U_1$ and $c\in R^*$, then

$$\theta(cab^{-1}c^{-1})=\theta(ca(cb)^{-1})=(cb-ca)(cb)^{-1} \tag{II.35}$$

$$=c(b-a)b^{-1}c^{-1}=c(ab^{-1})\theta(c^{-1}). \tag{II.36}$$

Thus we have

$$\theta(cxc^{-1})=c\theta(x)c^{-1} \tag{II.37}$$

for all $x\in U_1$ and $c\in R^*$; by continuity, (II.37) holds for $c\in R^*$ and any $x\in G_1$. Replacing x by $c^{-1}xc$ in (II.37) we obtain $\theta(x)=c\theta(c^{-1}xc)c^{-1}$, i.e.

$$\theta(c^{-1}xc)=c^{-1}\theta(x)c\quad(c\in R^*,\ x\in G_1). \tag{II.38}$$

Combining (II.37) and (II.38) we have

$$\theta(ab^{-1}x(ab^{-1})^{-1})=ab^{-1}\theta(x)(ab^{-1})^{-1}\quad(x\in G_1,\ a,\ b\in R^*),$$

and hence, again by continuity,

$$\theta(yxy^{-1}) = y\theta(x)y^{-1} \quad (x \in G_1, y \in G).$$

(ii) Let $ab^{-1} \in U_1$, then $a \neq b$ and $\theta(ab^{-1}) = (b-a)b^{-1}$, hence

$$\theta^2(ab^{-1}) = \theta((b-a)b^{-1}) = ab^{-1}.$$

Thus, (ii) holds on U_1, and by continuity on G_1.

(iii) Similarly, we have

$$\begin{aligned}\theta(ba^{-1}).ab^{-1}(\theta(ab^{-1}))^{-1} &= (a-b)a^{-1}ab^{-1}b(b-a)^{-1} \\ &= (-(b-a))(b-a)^{-1} = e;\end{aligned}$$

hence $\theta(x^{-1})x\theta(x)^{-1} = e$ for any $x \in G_1$,i.e. (iii) holds.

(iv) We first note that for any $c \in R^*$, the set $cR^*R^{*-1} := \{cab^{-1} : a, b \in R^*\}$ is dense in G. For, given $u \in G$ and $n \in \mathbb{N}$, there exist $a, b \in R^*$ such that $u \equiv ab^{-1} \pmod{K_n}$. If x and y are chosen in R^* to satisfy $ax \equiv cy \pmod{K_n}$ then $ab^{-1} \equiv cy(bx)^{-1} \pmod{K_n}$ and hence

$$u \equiv cy(bx)^{-1} \pmod{K_n}$$

with $cy(bx)^{-1} \in cR^*R^{*-1}$. Similarly $R^*R^{*-1}c^{-1} := \{ab^{-1}c^{-1} : a, b \in R^*\}$ is dense in G. Now let $x, y \in G_1$ $(x \neq y)$. We can find a sequence $(c_nd_n^{-1})$ in U_1 which converges to y and elements a_n, $b_n \in R^*$ such that $a_n \neq c_nb_n$, $a_n \neq d_nb_n$ and $a_n(d_nb_n)^{-1} \longrightarrow x$. If we put $(a_n(d_nb_n)^{-1} = x_n$ and $c_nd_n^{-1} = y_n$, then $(x_ny_n^{-1} = a_n(c_nb_n)^{-1}$ and by direct verification we get

$$\theta(x_ny_n^{-1}) = \theta[\theta(x_n)\theta(y_n)^{-1}].\theta(y_n^{-1}),$$

As $n \longrightarrow \infty$, $x_n \longrightarrow x$, and $y_n \longrightarrow y$, hence

$$\lim_{n \longrightarrow \infty} \theta(x_n)\theta(y_n)^{-1} \neq 1,$$

and we obtain

$$\theta(xy^{-1}) = \theta[\theta(x)\theta(y)^{-1}].\theta(y^{-1}).$$

So, condition (iv) holds.

Thus all conditions of lemma II.4.7 (page 86) are satisfied; hence we obtain a skew field $K := G \cup 0$ whose multiplicative group is G, where 0 is the zero element of R. Then R, as multiplicative semigroup, is a subsemigroup of K. Let us denote the subtraction in K by $x \boxminus y$ for the moment. By lemma II.4.7, we have

$$1 \boxminus x = \theta(x) \quad (x \neq 0, 1).$$

In particular, if $x := ab^{-1} \in U_1$, then

$$1 \boxminus ab^{-1} = \theta(ab^{-1}) = (b - a)b^{-1}.$$

Multiplying both sides by b on the right, we find

$$b \boxminus a = b - a. \tag{II.39}$$

If $a = b$, then the two sides of (II.39) are 0; for $b = 0$ they reduce to $-a$, by definition of e, while for $a = 0$ they both reduce to b. Thus (II.39) holds for all $a, b \in R$. Hence the additive group of R is a subgroup of the additive group of K, i.e. R is a subring of K. ∎

We shall now introduce some machinery and reformulate the hypothesis of theorem II.6.1 (page 92) in order to rewrite it in a suitable way for the applications we shall present.

Let R be a **filtered ring**, by this we mean a ring with a **filtration**, i.e. a

ring with a descending series

$$\ldots \supseteq R_{-1} \supseteq R_0 \supseteq R_1 \supseteq \ldots$$

of submodules such that

$$\bigcap_{n\in\mathbb{Z}} R_n = 0; \quad \bigcup_{n\in\mathbb{Z}} = R, \text{ and } R_m R_n \subseteq R_{m+n} \ (m, n \in \mathbb{Z}).$$

Then, we can define a function v on R by putting

$$v(x) = sup\{n : x \in R_n\}; \tag{II.40}$$

v satisfies the properties V.1, V.3 of valuations, while V.2 is replaced by

$$V.2' \qquad v(xy) \geq v(x) + v(y).$$

Thus, we have a **pseudo–valuation** on R. Conversely, any ring R with a pseudo–valuation v may be filtered by the submodules

$$R_n := \{x \in R : v(x) \geq n\}. \tag{II.41}$$

Now, with a filtered ring R there is associated a graded ring $G(R)$, an **associated graded ring**[9] of R, whose additive group is the direct sum

$$\bigoplus_{n\in\mathbb{Z}} (R_n/R_{n+1})$$

and whose multiplication is induced by that of R. By direct verification, we have that the function $v(x)$ defined on a filtered ring R by (II.40) is a valuation iff the graded ring $G(R)$ has no zero–divisors. In this case the hypothesis of

[9] Cf. Zariski and Samuel [ZS60].

theorem II.6.1 (page 92) may be reformulated as follows.

Theorem II.6.3 *Let R be a ring with a valuation v; then the following three conditions are equivalent:*

(i) For any $a, b \in R^*$ there exist $x, y \in R^*$ such that

$$v(ax - by) > v(ax),$$

(ii) for any $a, b \in R^*$, the function

$$f(x, y) = v(ax - by) - v(ax) \tag{II.42}$$

is unbounded above,

(iii) the graded ring $G(R)$ associated with R satisfies the Ore conditions.

Proof. We note that (i) is a special case of (ii); (i) also follows from (iii), for if $a, b \in R^*$ and $\overline{a}, \overline{b}$ are the corresponding elements of $G(R)$, then by (iii) there exist $x, y \in R^*$ such that

$$\overline{ax} - \overline{by} = 0,$$

i.e. $v(ax - by) > v(ax)$. To complete the proof it remains to show that (i) only if (ii) and (iii).

(i) only if (ii). Let $a, b \in R^*$ and suppose that the function $f(x, y)$ given by (II.42) is bounded; let $x, y \in R^*$ be such that $f(x, y)$ has its maximum value. If $c = ax - by$, then $c \neq 0$, because $v(c) - v(ax)$ is finite. By (i), there exist $u, v \in R^*$ such that $v(cu - bv) > v(cu)$, i.e.

$$v(axu - b(yu + v)) > v(axu - byu).$$

If follows that

$$v(axu - v(yu + v)) - v(axu) > v(axu - byu) - v(axu) = v(ax - by) - v(ax);$$

thus

$$f(xu, yu + v) > f(x, y),$$

which contradicts the definition of x, y. (i) only if (iii). Let $a, b \in G(R)$, say

$$a = a_{k+1} + \cdots + a_{k+r},$$
$$b = b_{l+1} + \cdots + b_{l+s},$$

where $a_i, b_i \in R_i/R_{i+1}$ and $a_{k+1}, a_{k+r}, b_{l+1}, b_{l+s}$ are all different from zero. When $r+s \leq 2$, the result holds by hypothesis, so we may assume that $r+s > 2$ and use induction on $r+s$; further we may assume that $r \leq s$, without loss of generality. By hypothesis there exist homogeneous elements $x, y \in G(R)$ which are not zero and satisfy

$$a_{k+1}x = b_{l+1}y.$$

The elements $a_{k+1}x$ is again homogeneous and belongs to R_m/R_{m+1} say; since $r \leq s$, the only degrees for which $ax - by$ can have non–zero terms are $m+1, \ldots, m+s-1$. By the induction hypothesis $ax - by$ and a have a non–zero common right multiple, say

$$(ax - by)u = av \neq 0;$$

hence $a(xu - v) = byu$, and this is not zero because $b, y, u \in G(R)^*$. Thus (iii) holds. ∎

We can now rewrite theorem II.6.1 (page 92) as follows:

Theorem II.6.4 *If R is a filtered ring such that the associated graded ring $G(R)$ satisfies the Ore conditions, then R can be embedded in a skew field.*

Proof. For when R is as stated, $G(R)$ has no zero–divisors, and therefore the filtration on R leads to a valuation; now we reach the conclusion by applying first theorem II.6.3 and then theorem II.6.1. ∎

II.7 Birkhoff–Witt algebras

An associative algebra A over a commutative field F is said to be a **Birkhoff–Witt algebras (BW–algebra** for short) if it has a filtration

$$0 = A_{-1} \subseteq A_0 \subseteq A_1 \subseteq \dots$$

such that the associated graded algebra $\bigoplus_{n \geq -1} (A_n/A_{n-1})$ is isomorphic–as graded algebra–to a polynomial ring in a number of indeterminates over F. A polynomial ring, being commutative, clearly satisfies the right Ore conditions, hence by theorem II.6.4, every BW–algebra can be embedded in a skew field. We need only put

$$R_n := A_{-n} \quad (A_{-1} = A_{-2} = \dots = 0)$$

to reach agreement with the notation used in section II.6.

For all the background material required in what remains of this section, see, for instance, Bourbaki [Bou75] or Jacobson [Jac62]. Let A be a BW–algebra over F; then $A_0 \cong F$, as F–algebras and if e is the element of A_0 which corresponds to the unit–element of F under this isomorphism, while u_λ $(\lambda \in \Lambda)$ is a set of elements of A_1 whose residue–class *mod* A_0 form a basis of A_1/A_0, then A is generated by the elements e and u_λ $(\lambda \in \Lambda)$ with the relations

$$e^2 = e, \tag{II.43}$$

$$eu_\lambda = u_\lambda + \alpha_\lambda e, \tag{II.44}$$

$$u_\lambda e = u_\lambda + \beta_\lambda e, \tag{II.45}$$

$$u_\lambda u_\mu - u_\mu u_\lambda = \sum \gamma^\nu_{\lambda\mu} u_\nu + \epsilon_{\lambda\mu} e, \tag{II.46}$$

where α_λ, β_λ, $\gamma^\nu_{\lambda\mu}$, $\epsilon_{\lambda\mu} \in F$. If we multiply (II.44) by e on the left and use (II.43)

we obtain

$$eu_\lambda = eu_\lambda + \alpha_\lambda e,$$

hence $\alpha_\lambda = 0$ and similarly $\beta_\lambda = 0$. Thus e is the unit–element of A and will henceforth be denoted by 1. Now (II.46) shows that *mod* A_0, A_1 admits the operation

$$[x, y] = xy - yx; \tag{II.47}$$

thus (II.47) may be used to define a bilinear multiplication on the space A_1/A_0. By direct verification (which will be omitted) one sees that the resulting linear algebra is a **Lie algebra**[10] with basis u_λ ($\lambda \in \Lambda$) and structure constants $\gamma^{\nu}_{\lambda\mu}$. We denote this Lie algebra by L and on L define a bilinear form $b(.,\ .)$ by putting

$$b(u_\lambda, u_\mu) := \epsilon_{\lambda\beta}.$$

If follows from (II.46) and the linear independence of u_λ and e that b is an alternating form, i.e.

$$b(x, x) = 0 \quad (x \in L).$$

If we denote the multiplication in L by $[xy]$, we can rewrite (II.46) as

$$xy - yx = [xy] + b(x, y)1 \quad (x, y \in L), \tag{II.48}$$

and using this relation to express the **Jacobi–identity** in L we find that

$$b([xy], z) + b([yz], x) + b([zx], y) = 0. \tag{II.49}$$

An alternating bilinear form will be called a **2–cocycle** if it satisfies (II.49). Thus any BW–algebra A leads to a Lie algebra L with a 2–cocycle alternating

[10] Cf. Jacobson [Jac62].

bilinear form b defined on it, and A is completely determined by L and b.

Conversely, let L be any Lie algebra over F with a 2–cocycle alternating bilinear form b defined on it. Then the associative algebra with unit–element 1 which is generated by the elements of L with the relations (II.48) is a BW–algebra which in turn leads to L with b as its 2–cocycle form. For the special case $b = 0$ this is the classic **Poincare–Birkhoff–Witt theorem**[11], the proof in the general case is entirely analogous, cf. Jacobson or Bourbaki (loc. cit.).

We shall denote the BW–algebra for a given Lie algebra L with a 2–cocycle form b by $A(L; b)$. As special cases we note:

1. The enveloping algebra of a Lie algebra L, namely, $A(L; 0)$.

2. The free associative algebra K, say, over F on $x_1, \ldots, x_r$ as free set of generators. K may be regarded as a Lie algebra, using the operation (II.47), and if L is the Lie algebra (in this sense) generated by $x_1, \ldots, x_r$ then $K \cong A(L; 0)$. Taken together with theorem II.6.4 (page 104), this provides, yet, another proof of the fact that K may be embedded in a skew field.

[11] Cf. Birkhoff [Bir37] and Witt [Wit37].

CHAPTER III

A general method of embedding

In this chapter we shall see a general method [Coh71a, Coh72a, Coh72b, Coh85] of embedding rings in skew fields due to Cohn. This technique is quite general in that it provides a criterion for arbitrary rings to be so embeddable, and also can be used to describe the homomorphisms of rings into skew fields. For a commutative ring such homomorphisms can be completely described in terms of the set of its prime ideals, and in the course of this chapter we shall see that the same description applies to non–commutative rings.

Let R be a ring. Our basic problem will be to study the possible ways of embedding R into a skew field. Of course there may be no such embedding, and it is more natural to treat the wider problem of finding homomorphisms of R into a skew field. Even this problem may have no solution, e.g. if $R = K_n$ is a matrix ring over a skew field, where $n > 1$, then R is simple (since K is), so any homomorphism f of R into a field must be injective (f can not be zero, because $f(1) = 1 \neq 0$), and this is impossible because R has zero–divisors.

As a possible step towards the solution we may take a subset T of R and

consider T–inverting homomorphisms, as we did in chapter I (where we were "protected" under the Ore conditions). As we saw in corollary I.3.12, page 28, in the Ore case, once we have an R^*–inverting homomorphism, we have achieved the embedding in a field (we even have a unique field of fractions with a prescribed normal form). Assume that K is the field of fractions of an Ore domain R. Then, every element u of K can be written as $a^{-1}b$ ($a, b \in R$). Thus, u is obtained by solving

$$au - b = 0. \tag{III.1}$$

But in general, if we have an R^*–inverting homomorphism, we do not necessarily get an embedding into a skew field; after adjoining the inverses of all non–zero elements of R, there may still be elements without inverses, e.g. $ab^{-1}c + de^{-1}f$ (recall that now we don't have the right multiple condition to "shuffle elements around"), so we need to perform repeated inversions.

Thus, for a non–commutative ring R the R^*–inverting homomorphisms are not very good approximations to homomorphisms into a skew field. Following Cohn, we shall remedy this defect by inverting, instead of elements, a set of square matrices over R (possibly of different orders) and we shall be able to manage with a single inversion ("to invert them all in one step") if we replace a in (III.1) by a matrix. Since our aim is to construct skew fields, we shall confine ourselves to square matrices, the only ones that can be inverted over a field (since any field has invariant basis number).

For a commutative ring this gives nothing new, since we can invert any square matrix A simply by adjoining an inverse of $det\ A$ (the determinant of A). But over a non–commutative ring, although a determinant can be defined, it lacks the properties required to achieve an analogous situation to the commutative case, so we expect the inverse of a matrix to give something new. We shall see that this new ingredient will lead us to the solution of our problem: we want to characterize the homomorphisms from R to skew fields by means of

"structure" defined over R (this structure will be the prime matrix ideal of R, to be defined below). Then constructing such structure on R will be "equivalent" to constructing a homomorphism to a skew field.

Here we shall regard skew field extensions as irrelevant, so that a homomorphism to a skew field composed with an inclusion map into a larger skew field is the same (for our purposes) as the original homomorphism (for instance, think on $\mathbb{Z}$, the integers, which is embedded in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{H}$; we shall be particularly interested in the "epic" $\mathbb{Z}$–fields $\mathbb{Q}$ that is generated as a field by $\mathbb{Z}$).

For example, if R is a commutative ring, a homomorphism from R to an "epic" field K is determined by the kernel p, a prime ideal in R. K must be commutative because being "epic", it is generated as a field by (the commutative ring) R. Then K and the homomorphism may be constructed from the prime ideal in two different ways: forming the factor ring R/p (an integral domain since p is prime) and then K is obtained as the field of fractions of R/p; or forming the localization R_p, this is a local ring and its residue class field is isomorphic to K. The former method does not seem to generalize to the non–commutative case, but we shall see that the latter does.

We shall be interested in R–rings that are skew fields, called R–fields. We shall single out a particular class of R–fields, the epic R–fields, and shall introduce a category having epic R–fields for objects and as morphisms certain equivalence classes of local homomorphisms called specializations (the justification for looking at the epic R–fields and not all the R–fields will become clear later, cf. page 129). In order to construct epic R–fields we shall introduce the concepts of singular kernel and universal Σ–inverting ring R_Σ (here Σ is a set of square matrices over R, possibly of different orders). To form the universal Σ–inverting ring R_Σ, essentially means to adjoin to R the entries of the inverses of the matrices of Σ in the most general way possible.

A basic step in the construction of an epic R–field is the description of its elements as components of the solution vector of a matrix equation. Towards

this end we shall introduce the Σ–rational closure of R with respect to a ring homomorphism from R to another ring. When Σ happens to be "multiplicative", we shall give a characterization of the Σ–rational closure of R, which is at the basis of all further development. Then we prove a sort of Cramer's rule for non–commutative rings. We also prove lemma III.2.3, on page 127, which is original. It will give us the exact relation between the universal Σ–inverting ring and the Σ–rational closure. As an application of Cramer's rule and this lemma we shall show how to construct epic R–fields from their singular kernels. It will turn out that when Σ consists of all square matrices over R which become invertible over an epic R–field K, then R_Σ will be a local ring with residue–class field K; and conversely, if Σ is such that R_Σ is a local ring, then its residue class field will be an epic R–field. (cf. page 129).

From the above discussion, we shall have known that any epic R–field may be described entirely in terms of matrices over R; we shall also see how to express specializations in terms of the sets of matrices inverted over R: there is a specialization between two epic R–fields iff there is an inclusion relation between their singular kernels. This will give us an equivalence between the category of epic R–fields and specializations and the category whose objects are singular kernels of epic R–fields with inclusion mappings as morphisms.

At this stage, we would like to know when a collection of matrices is a singular kernel, just as we can tell when a collection of elements of R is a prime ideal. In fact we shall be able to characterize singular kernels in much the same way as kernels of R–fields in the commutative case are characterized as prime ideals. To this end we introduce some operations on the set of matrices over R and the notion of a matrix ideal. This corresponds to the concept of an ideal in a commutative ring. Then, we shall define the analogue of a prime ideal: the prime matrix ideal, which has properties corresponding closely to those of prime ideals. Prime matrix ideals can be used to describe homomorphisms of general rings into skew fields, just as prime ideals do in the commutative

case. Given a homomorphism of R into an epic field K, we may apply this homomorphism to matrices over R (i.e. with entries in R) by applying the homomorphism to each entry. Then the prime matrix ideal of R determined by this homomorphism consists of those square matrices over R whose images under the homomorphism are singular over K. This collection of matrices actually determines the homomorphism (up to isomorphism). Always keep in mind the analogy with the commutative case: for a commutative ring R, the prime ideals are the set of elements of R which become 0 under a homomorphism into some field. Thus, the crux of this chapter is the following

characterization of prime matrix ideals: prime matrix ideals are the sets of square matrices over R which become singular under a homomorphism into some skew field.

This characterization of prime matrix ideals will be applied to derive criteria for a general ring to be embeddable in a field, or to have a universal field of fractions.

These results may be used to show that every "semifir" has a universal field of fractions. In particular, since

- free algebras over a commutative field,
- group algebras of free groups over a commutative field,
- free products of skew fields over a common subfield

are semifirs, they will be embeddable in skew fields.

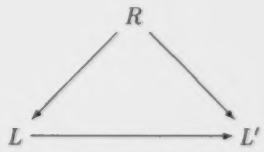
An alternative approach to the method of universal localization was given by Gerasimov [Ger79, Ger82]. Gerasimov put emphasis in studying homomorphisms of rings into rings (not necessarily skew fields) and characterized all such mappings. His work lead to a localization theorem for n–firs. This theorem was proved independently by Malcolmson [Mal84], who simplified some of the proofs of this chapter, cf. [Mal78, Mal80, Mal82, Mal84].

We also mention that Schofield [Sch85] generalized Cohn's method of embedding rings into skew fields and studied finite dimensional representations of a ring over a skew field. An alternative view of this is that he classified all possible homomorphisms from a ring to simple artinian rings. In this set up, it can be said that such a study was carried out, in the case of one dimensional representations which are simply homomorphisms to skew fields, by Cohn, Gerasimov and Malcolmson.

III.1 The category of epic R–fields and specializations

Given a ring R, by an **R–ring** we understand a ring L with a ring homomorphism $R \longrightarrow L$ called the **canonical homomorphism** of L.

For fixed R, the R–rings form a category (the comma category[1] of R over the category of rings) in which the morphisms, called **R–ring homomorphisms** are the ring–homomorphisms $L \longrightarrow L'$ such that the triangle shown is commutative. ∎



An R–ring that is a field is called an **R–field**. Of course for some rings R there will be no R–fields at all, e.g. $R = 0$ (recall that in a field $1 \neq 0$), or for a less trivial example, any simple ring with zero–divisors, say a matrix ring R over a skew field. For any map $R \longrightarrow K$ must be injective and this is impossible when K is a field. Even entire rings R without R–fields exist, e.g. if R is any ring without invariant basis number (cf. [Coh66]); R may be choosen entire and any R–ring is again without invariant basis number and so can not be a field.

[1] Cf., for instance, Herrlich and Strecker [HS73] or Mac Lane [ML71]

We shall be interested in **epic R–fields**, i.e. R–fields that are generated as fields by the image of R ($\mathbb{Q}$ is an epic $\mathbb{Z}$–field, and $\mathbb{R}$ and $\mathbb{C}$ are $\mathbb{Z}$–fields that are not epic; $\mathbb{Z}_p$, p a prime in $\mathbb{Z}$, is an epic $\mathbb{Z}$–field).

Recall that a ring homomorphism $f : R \longrightarrow S$ is **epic** in the category of rings if it is right cancellable, i.e. given two ring homomorphisms α, β from $S \longrightarrow T$ (T a ring), if $\alpha f = \beta f$ then $\alpha = \beta$. The following fact justifies why we call them *"epic"* R–fields: **if K is an epic R–field then the canonical map R $\longrightarrow$ K is epic in the category of rings**. Indeed, let K be an epic R–field with canonical homomorphism $\mu_K : R \longrightarrow K$. Assume given two ring homomorphisms α, β from $K \longrightarrow T$ (T a ring), and that $\alpha\mu_K = \beta\mu_K$. Then, α and β agree on the image $\mu_K(R)$, but since K is an epic field, it is generated, as a field, by $\mu_K(R)$, hence, being α and β ring homomorphisms, they must agree in the whole of K. ∎

If K is an epic R–field for which the canonical map $R \longrightarrow K$ is injective, K is called a **field of fractions** of R, cf. definition I.3.6, page 21 ($\mathbb{Q}$ is a field of fractions for $\mathbb{Z}$, $\mathbb{Z}_p$ is not a field of fractions for $\mathbb{Z}$. Actually, being $\mathbb{Z}$ Ore, $\mathbb{Q}$ is the unique field of fractions of $\mathbb{Z}$, cf. proposition I.3.15, page 30).

Our goal, now, is to make the epic R–fields (for a given ring R) the objects of a category, so we must find the "appropriate" morphisms. The only R–ring homomorphism between epic R–fields is an isomorphism. For any homomorphism between fields must be injective (because the kernel is a proper ideal of a field), and in this case the image will be a field containing the image of R, hence we have a surjection (because L was epic), and so an isomorphism. This shows the need to consider more general maps.

Given any R–ring A, by an **R–subring** of A we mean a subring A_0 of A which contains the image of R under the canonical homomorphism of A. So, A_0 is also an R–ring. By a **local R–subring** we mean an R–subring A_0 which is a local ring, i.e. the non–units of A_0 form an ideal of A_0.

To obtain a workable notion of morphism let us define a **local homomor-**

phism between any R–rings A, B as a R–ring homomorphism $f : A_0 \longrightarrow B$ whose domain A_0 is an R–subring of A and which maps non–units to non–units.

If B is a field, this means that the non–units in A_0 form an ideal, namely $ker\ f$, hence A_0 is then a **local ring**, i.e. a ring A_0 in which the non–units form an ideal, say $\mathfrak{m}$; the quotient ring $A_0/\mathfrak{m}$ is then a field (since the non–zero elements in it already had a unit in A_0), called the **residue–class field** of A_0.

Note, in particular, that a local homomorphism between R–fields K, L is an R–ring homomorphism $f : K_0 \longrightarrow L$ whose domain K_0 is a R–subring of K such that any element of K_0 not in the kernel of f has an inverse in K_0 (because the only non–unit of a field is zero), in other words, a local homomorphism between R–fields "kills" (sends to zero) every non–unit of its domain which is a local R–subring of the source R–field. By what has been said, K_0 is a local ring with residue class field $K_0/ker\ f \cong Imf$; so Imf is a subfield of L containing the image of R under the canonical homomorphism of L, and hence, *if L is epic*, equal to L. Thus,

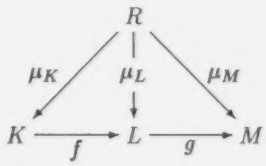
(III.2) $$K_0/ker\ f \cong Imf = L, \text{ if } L \text{ is epic.}$$

Therefore, **any local homomorphism to an epic R–field is surjective**.

Now, let's agree when we shall consider two local homomorphisms "equal". Two local homomorphism from an R–field K to another one, L, are **equivalent** if they agree on a subring K_0 of K and the common restriction to K_0 is again a local homomorphism, this simply means that K_0 is an R–subring of K such that every element of K_0 not in the kernel of the common restriction has an inverse in K_0. This is easily verified to be an equivalence relation in the set of all local homomorphisms between R–fields; now a **specialization** between two epic R–fields K and L is defined as an equivalence class of local homomorphisms from K to L.

The R–fields and specializations form a **category $\mathcal{F}_R$**, say. Here it is only

necessary to check that the composition of maps is defined:



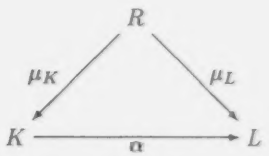
given specializations $f : K \longrightarrow L$, $g : L \longrightarrow M$, (keep in mind that f and g are not functions, they are equivalence classes of local homomorphism; but without fear of confusion, we shall denote by f and g a representative of the equivalence classes f and g, respectively) let K_0, L_0 be the domains of f and g, respectively, and put $K_1 = \{x \in K_0 : f(x) \in L_0\}$, $f_1 := f|K_1$. We assert that $gf_1 : K_1 \longrightarrow M$ is a local homomorphism and so defines a specialization (namely, its equivalence class). To see this, let us denote the canonical mapping $R \longrightarrow K$ by μ_K; then we have $f\mu_K = \mu_L$, hence $\mu_K(R) \subseteq K_1$, so that K_1 is an R–ring. Moreover, if $x \in K_1$ and $gf_1(x) \neq 0$, then $f(x) = f_1(x) \neq 0$, so $x^{-1} \in K_0$ and $f(x^{-1}) = f(x)^{-1} \in L_0$, hence $x^{-1} \in K_1$. This shows that gf_1 defines in fact a specialization.

At first sight it looks as if there may be several specializations between a given pair of epic R–fields. For example, let $R := k[x, y]$ be the commutative polynomial ring over a skew field, $K := k(x, y)$ its field of fractions with the natural embedding and $L := k$ with the homomorphism $R \longrightarrow L$ given by $x \mapsto 0$, $y \mapsto 0$. We obtain a specialization from K to L by defining a homomorphism $\alpha : k[x, y] \longrightarrow L$ in which $\alpha(x) = \alpha(y) = 0$. Let K_0 be the localization of $k[x, y]$ at the maximal ideal (x, y), then α can be extended in a natural way to K_0. We observe that there are local homomorphisms from K to L that are defined on larger local subrings than K_0 (for instance, we can "specialize" rational functions $\phi(x, y)$ so that x/y takes on a specified value in k), but all agree on K_0, so that there is just one specialization from K to L.

In fact this is a general property:

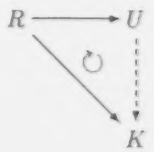
Lemma III.1.1 *Between any two epic R–fields can be at most one specialization.*

Proof.



Assume, given any two epic R–fields, K and L, with a specialization $\alpha: K \longrightarrow L$. Being K an epic field, μ_K must be epic in the category of rings (cf. page 114), and hence so is any corestriction of μ_K. Then, the result follows from the commutativity of the above triangle. Indeed, let $\beta: K \longrightarrow L$ be another specialization. By definition of specialization, we have that $dom(\alpha) \cap dom(\beta) \supseteq \mu_K(R)$ and then, the corestriction $R \xrightarrow{\mu_K} dom(\alpha) \cap dom(\beta)$ must be epic, and since $\beta \circ \mu_K = \mu_L$ and $\alpha \circ \mu_K = \mu_L$, then $\beta = \alpha$, i.e. β and α agree on their common restriction, so as specializations they are equal. ∎

Let $\mathcal{E}_R$ be the full subcategory of $\mathcal{F}_R$ whose objects are the epic R–fields. An initial object in $\mathcal{E}_R$ is called a **universal epic R–field**.



Explicitly, a universal epic R–field is an epic R–field U such that for any epic R–field K there is a unique specialization $U \longrightarrow K$. Clearly a universal R–field, if it exists at all, is unique up to isomorphism.

In general a ring R need not have a universal epic R–field (e.g. a commutative ring has a universal epic R–field iff its nil radical is prime [Hun89], page 379 and we shall obtain a condition for general rings later on, cf. corollary III.3.2, page 133). Suppose that R has a universal epic R–field U; then R has a field

of fractions iff U is a field of fractions, as a glance at the above triangle shows. In that case we call U the **universal epic field of fractions**. An example of G. M. Bergman (cf. [Coh72a], page 37) shows that the existence of a universal epic R–field and of a field of fractions are quite independent: neither entails the other.

Let us give some examples to illustrate these definitions and to see how the category $\mathcal{E}_R$ of epic R–fields look like in particular cases.

1. Let R be a (left or right) Noetherian ring. Any epic R–field is obtained as a field of fractions of $R/\mathfrak{a}$ for a suitable ideal $\mathfrak{a}$. But $R/\mathfrak{a}$ is again Noetherian and an integral domain, as a subring of a field, and hence (by proposition I.3.14, page 29) it is left or right Ore domain and the field of fractions of $R/\mathfrak{a}$ is unique up to isomorphisms (cf. proposition I.3.15, page 30). Let us call an ideal $\mathfrak{a}$ **completely prime** or **strongly prime** if $R/\mathfrak{a}$ is an integral domain; what has been said shows that the category of $\mathcal{E}_R$, for a left or right Noetherian ring, is isomorphic to the category whose objects are the completely prime ideals of R, with inclusions maps as morphisms.

2. Let R be a commutative ring. Then, every epic R–field is also commutative. The epic R–fields correspond precisely to the prime ideals of R. Thus, given any epic R–field K, the kernel of the canonical homomorphism $\mu_K : R \longrightarrow K$ is a prime ideal, and conversely, if $\mathfrak{p}$ is a prime ideal of R, then the mapping $R \longrightarrow F(R/\mathfrak{p})$ (where $F(A)$ denotes the field of fractions of A, A a commutative integral domain) gives us an epic R–field. The category $\mathcal{E}_R$ of epic R–fields is isomorphic to the category whose objects are the prime ideals of R, with inclusions maps as morphisms. There is a universal R–field iff there is a least prime ideal, i.e. the nil radical is prime, and when this is 0 (i.e. when R is a commutative integral domain), we have a universal field of fractions. A similar correspondence exists in the general case, and will be described later cf. page 130, once we have identified the objects to be used in place of prime ideals (namely, "prime matrix ideals" and recall that the crux of this chapter

is to characterize prime matrix ideals as the sets of square matrices over R which become "singular" under a homomorphism into some skew field, i.e. the "singular kernels").

To find what we need, let us consider a general epic R–field K with canonical homomorphism $\mu_K : R \longrightarrow K$. Writting $\ker \mu_K = \mathfrak{p}$, we have the following commutative diagram.

$$\begin{array}{ccc} R & \longrightarrow & R_{\mathfrak{p}} \\ \downarrow & \searrow^{\mu_K} & \downarrow \\ R/\mathfrak{p} & \longrightarrow & K \end{array}$$

When R is commutative, then so is K (being generated by a homomorphic image of R) and $\mathfrak{p}$ is a prime ideal of R which determines K up to isomorphism. We can construct K in two ways. Firstly, we can form $R/\mathfrak{p}$, an integral domain (because $\mathfrak{p}$ is prime), and now K is obtained as the field of fractions of $R/\mathfrak{p}$. Secondly, instead of putting the elements of $\mathfrak{p}$ equal to zero, we can make the elements outside $\mathfrak{p}$ invertible, by forming the localization $R_{\mathfrak{p}}$. This is a local ring and its residue–class field is isomorphic to K. In the general case $\mathfrak{p}$ is no longer sufficient to determine K, since as we saw in section I.6, page 46, there are rings with several non–isomorphic field of fractions.

Thus to describe an epic R–field we need more than the elements which map to zero, we need the matrices which become "singular". Here we use the fact that for any square matrix A over a field K (even skew) the following four conditions are equivalent (cf. [Hun89], page 342):

A has no left or right inverse,

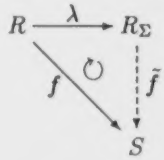
A is a left or right zero–divisor.

A matrix A over a skew field with these properties is called **singular**.

Let us use the following notation: given a ring homomorphism $f : R \longrightarrow S$ and a matrix A with entries in R (we shall say, as usual, A is "over R"), then $f(A)$ will denote the matrix over S each of whose entries is obtained by applying the homomorphism f to the corresponding entry of A.

Let Σ be a set of square matrices over a ring R, possibly of different orders. A homomorphism $f: R \longrightarrow S$, S a ring, is said to be a **Σ–inverting homomorphism** if every matrix in Σ is mapped by f (applied to each entry of the matrix) to an invertible matrix in S.

Our aim will be to study the epic R–field K by means of the set of all square matrices over R which become invertible over K under the canonical homomorphism of K; before we can do so, we need the important remark that for any set Σ of square matrices over R, there always exists a **universal Σ–inverting homomorphism**: by this term we understand a homomorphism $\lambda: R \longrightarrow R_\Sigma$, into some ring R_Σ which is Σ–inverting and such that any Σ–inverting homomorphism f can be factored uniquely by λ, i.e. given any $f: R \longrightarrow S$ such that $f(\Sigma)$ consists of invertible matrices, there is a unique homomorphism $\tilde{f}: R_\Sigma \longrightarrow S$ such that the accompanying triangle commutes.



The ring R_Σ is clearly determined up to isomorphism by these conditions; it is called the **universal Σ–inverting ring** or also a **universal localization** of R.

Such a ring always exists (for any choice of R and Σ, even if the matrices of Σ are not square, but since we are interested in homomorphisms into skew fields, we shall restrict our attention to square matrices, cf. Gerasimov [Ger79, Ger82] for a more general situation) and it may be constructed as follows. For each $m \times m$ matrix $A = (a_{ij})$ in Σ we take a set of m^2 symbols, arranged as an $m \times m$ matrix $A' = (a'_{ji})$ and take a ring presentation of R_Σ consisting of all the elements of R, as well as all the a'_{ji} as generators, and as defining relations

take all the relations holding in R, together with the relations, in matrix form,

(III.3) $$AA' = A'A = I \qquad \text{for each } A \in \Sigma.$$

The mapping taking each element of R to the corresponding element of R_Σ is clearly a homomorphism $\lambda : R \longrightarrow R_\Sigma$, which is Σ–inverting , by construction. If $f : R \longrightarrow S$ is any Σ–inverting homomorphism, we define a homomorphism $\tilde{f} : R_\Sigma \longrightarrow S$ by putting $\tilde{f}(x) = f(x)$ for all $x \in R$ and for any matrix $A \in \Sigma$ defining $\tilde{f}$ on $\lambda(A)^{-1}$ by putting $\tilde{f}(\lambda(A)^{-1}) = f(A)^{-1}$. This gives a well defined homomorphism $\tilde{f}$, because any relation in R_Σ is a consequence of the defining relations in R and the relations III.3, and all these relations also hold in S.

Of course the canonical homomorphism $\lambda : R \longrightarrow R_\Sigma$ need not be injective (because there may be identifications between the elements of R in R_Σ due to the extra relations (III.3)) and may, in fact, be zero (for instance, if $R = 0$ or if $0 \in \Sigma$). However, from the commutative triangle above we already see that if there is a Σ–inverting homomorphism f which is injective, then λ must be injective. We sum up these results in

Theorem III.1.2 *Let R be any ring and Σ be a set of square matrices over R. Then there is a universal localization R_Σ, unique up to isomorphism, with a universal Σ–inverting homomorphism*

(III.4) $$\lambda : R \longrightarrow R_\Sigma.$$

Moreover, λ is injective iff R can be embedded in a ring over which all the matrices of Σ have inverses. ∎

Let us now consider, for an epic R–field K, in place of $\mathfrak{p} = ker\ \mu_K$, the set $\mathcal{P}$ of all square matrices over R (of all orders) which map to singular matrices over K under the canonical homomorphism of K. This set $\mathcal{P}$ is called the **singular kernel** of μ_K and is written $Ker\ \mu_K$ (note the capital letter in "Ker"). Al-

though there is no obvious construction for $R/\mathcal{P}$, "the ring obtained by putting the matrices in $\mathcal{P}$ equal to zero" (so one of the methods for constructing field of fractions in the commutative case is not at our disposal in the general case), we can still define a localization since we now have the universal Σ–inverting ring R_Σ at hands, where Σ will be the set of all square matrices over R which become invertible over K; or what is the same, the complement of $\mathcal{P}$ in the set $\mathcal{M}(R)$ of all square matrices over R.

We define a **localization $\mathbf{R_\mathcal{P}}$** (analogous as $R_\mathfrak{p}$ in the commutative case) as the universal Σ–inverting ring R_Σ, where Σ is the complement of $\mathcal{P}$ in the set $\mathcal{M}(R)$ of all square matrices over R. By abuse of language, although we are localizing at the set of square matrices over R which become invertible over K, we sometimes say that we localize at (its complement in $\mathcal{M}(R)$) the set of matrices over R which become singular over K, exactly as we do in the commutative case.

We can now describe the construction of an epic R–field in terms of its singular kernel. Let K be an epic R–field, $\mathcal{P}$ its singular kernel and Σ the complement of $\mathcal{P}$ in the set of all square matrices over R. Thus, we repeat that Σ consists of all square matrices over R which become invertible over K. Then, we claim that the universal Σ–inverting ring R_Σ is a local ring, with residue–class field K. We shall soon see a proof of this claim (cf. page 129), but we note that this does not solve our problem yet. For we would like to know when a collection of square matrices over R is a singular kernel, just as we can tell when a collection of elements of R is a prime ideal.

III.2 The construction of epic R–fields from their singular kernels

A basic step in the construction of an R–field is the description of its elements as components of the solution vector of a matrix equation.

Given a Σ–inverting homomorphism $f : R \longrightarrow S$, (S a ring) the set of all entries of matrices $f(A)^{-1}$, where $A \in \Sigma$, is called the **Σ–rational closure**, or simply, the **rational closure** if Σ is understood, under f of R in S.

We shall mainly be interested in the case where the Σ–rational closure is a ring (actually, a subring of S). So we shall give conditions on Σ for this Σ–rational closure to be a ring; in fact these restrictions correspond to the condition of being multiplicatively closed in the commutative case for sets of elements (keep always in mind the analogy with the commutative case, where the set of elements to be inverted is required to be a multiplicative set for convenience in defining addition and multiplication; later,we shall define operations in the set of matrices over a ring to characterize the singular kernels in a similar way as the kernels of ring homomorphisms from commutative rings into commutative field are characterized as prime ideals).

So we define a set Σ of square matrices over a ring R to be **multiplicative** if it includes the 1×1 matrix 1 and for any A, $B \in \Sigma$ we have

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \in \Sigma \quad \text{for all matrices } C \text{ of the right size.}$$

The following remark, though easy to prove, is fundamental. **For any ring homomorphism f : R $\longrightarrow$ S (S a ring) the set of all matrices inverted over S is always multiplicative**, for 1 is invertible and if A, B are invertible, so is $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$, with inverse

$$\begin{pmatrix} A^{-1} & -A^{-1}CB^{-1} \\ 0 & B^{-1} \end{pmatrix}.$$

Actually, any set of inverted matrices over S, containing 1, is always multiplicative.

We shall characterize the rational closure.

Theorem III.2.1 (Characterization of the rational closure) *Let R be a ring and Σ a multiplicative set of square matrices over R. Given a Σ–inverting homomorphism $f: R \longrightarrow S$ (S a ring) the following conditions are equivalent for any element $x \in S$:*

(a) x is an element of the Σ–rational closure under f of R in S,

(b) x is a component of the solution vector u of a matrix equation

(III.5)
$$Au + a = 0, \qquad \text{where } A \in f(\Sigma), \text{ and } a \text{ is a column over } f(R),$$

(c) x is a component of the solution vector u of a matrix equation

(III.6)
$$Au = e, \qquad \text{where } A \in f(\Sigma), \text{ and } e \text{ is a column of the identity matrix.}$$

Moreover, the set of all these elements x, i.e. the Σ–rational closure under f of R in S, is a subring of S containing $f(R)$.

Proof. Keep in mind that, by definition, the Σ–rational closure under f of R in S consists of the entries of the inverses of matrices in $f(\Sigma)$. (c) states that u is a column of A^{-1} (A^{-1} exists since $A \in f(\Sigma)$ and f is Σ–inverting), hence we have (c) iff (a). Note that (III.6) is a special case of (III.5), so we also have (c) only if (b).

To prove (b) only if (c) we note that if $Au + a = 0$, then

$$\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0,$$

so when (b) holds, each component satisfies an equation of type (III.6) (indeed,

note that $\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \in f(\Sigma)$ since Σ is multiplicative) and so (c) holds. So, all three conditions are equivalent.

To prove that the rational closure is a ring containing $f(R)$ we use (b): for any $c \in f(R)$ we obtain c as a solution of $1u - c = 0$, hence $f(R)$ is included in the Σ–rational closure under f of R in S. Now let u_i be the i–th component of the solutions of $Au + a = 0$ and v_j be the j–th component of the solution of $Bv + b = 0$, then $u_i - v_j$ is the first component of the solution of

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} w + \begin{pmatrix} a \\ b \end{pmatrix} = 0,$$

where C has for its j–th column the i–th column of A and the rest 0. Next $u_i v_j$ is the i–th component of the solution of

$$\begin{pmatrix} A & D \\ 0 & B \end{pmatrix} w + \begin{pmatrix} 0 \\ b \end{pmatrix} = 0,$$

where D has as its j–th column a and the rest 0. This shows that the Σ–rational closure under f of R in S is closed under subtraction and multiplication, and we have already seen that it contains 1, therefore it is a subring of S. ∎

Although there is no "effective" criterion for deciding when an element of the rational closure is zero, there is a useful method, to be described in theorem III.2.2 below, of recognising zero–divisors in the rational closure (which will be good enough for our purpose because we are interested in the case where S is a field and then the non–zero elements are the non–zero divisors, actually, the units of S); this will illustrate the fact that properties of the solution vector u of $Au + a = 0$ (or better of its components) can be expressed in terms of A and a.

Theorem III.2.1 shows that every element of the rational closure can be

obtained as some component u_i of the solution vector u of a matrix equation

$$Au = a.$$

Here A is called the **denominator** of u_i, and A_i, the matrix obtained by replacing the i–th column of A by a, is called the **numerator** of u_i. This terminology is justified by *Cramer's rule*, which states that when R is commutative,

$$u_i = -\frac{det\ A_i}{det\ A}.$$

In the general case we no longer have this formula (because we do not have determinants), but we have the following substitute, still called **Cramer's rule**:

Theorem III.2.2 (Cramer's rule for non–commutative rings) *Given a ring S, let u_i be the i–th component of the solution vector u of*

$$Au + a = 0, \tag{III.7}$$

where A is an invertible matrix over S of order n and a is a column vector over S of order n. Write $A = (a_1, \ldots, a_n)$ where a_i is the i–th column of A and let A_i be the matrix obtained by replacing the i–th column of A by a, so $A_i = (a_1, a_2, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n)$.

Then u_i is (i) a left zero–divisor, (ii) a right zero–divisor, (iii) left invertible or (iv) right invertible in S if and only if A_i has the corresponding property in $\mathcal{M}_n(S)$ (the ring of matrices over S of order n).

Further, $u_i = 0$ if and only if a is a right linear combination over S of the $n-1$ columns of A $a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$.

Proof. We prove the result for u_1, the case for u_i $(1 \leq i \leq n)$ follows similarly.

We first note that an element c of any ring has any of the properties (i)–(iv) iff any associate ucv has the corresponding property (where u, v are units).

Secondly, we note that A_1 is associated to $\begin{pmatrix} u_1 & 0 \\ 0 & I \end{pmatrix}$ in $\mathcal{M}_n(S)$ (where I is the identity matrix of order $n-1$ over S); for on writting $u = \begin{pmatrix} u_1 \\ u' \end{pmatrix}$, (where u' is the column vector form with the last $n-1$ components of u), we have

$$A_1 = A(A^{-1}A_1) = A\begin{pmatrix} u_1 & 0 \\ u' & I \end{pmatrix} = A\begin{pmatrix} u_1 & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} 1 & 0 \\ u' & I \end{pmatrix},$$

and here the outer factors on the right hand side of the right most equality are units in $\mathcal{M}_n(S)$. Finally, it is clear that u_1 has any one of the properties stated precisely when $\begin{pmatrix} u_1 & 0 \\ 0 & I \end{pmatrix}$ does.

To prove the last sentence we rewrite (III.7) as

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n + a = 0. \tag{III.8}$$

If $u_1 = 0$, (III.8) shows that a is a right linear combination of the last $n-1$ columns of A. Conversely, let $v_2, \ldots, v_n \in S$ be such that

$$a_2v_2 + + \cdots + a_nv_n + a = 0,$$

then (III.7) has the solution $(u_1, \ldots, u_n)^T$ (where T notes "transposed") and $(0, v_2, \ldots, v_n)^T$, hence by uniqueness of the solution of the system of linear equations (III.7) (recall that A is invertible), we have $u_1 = 0$. ∎

Having Cramer's rule at our disposal, we shall show how to construct epic R–fields from their singular kernels. But first, we need a corollary of the following lemma.

Lemma III.2.3 *Let R be a ring and and let Σ be a* multiplicative *set of square matrices over R. Consider the universal Σ–inverting ring R_Σ with universal*

Σ–inverting homomorphism $\lambda: R \longrightarrow R_\Sigma$. Let $\overline{\Sigma}$ be the Σ–rational closure of R in R_Σ under λ. Then, $\overline{\Sigma} = R_\Sigma$.

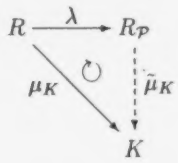
Proof. It follows from theorem III.2.1 that $\overline{\Sigma}$ is a subring of R_Σ that contains the image of R under λ, so $\lambda(R) \subseteq \overline{\Sigma}$. So to have the claimed equality, being $\overline{\Sigma}$ a subring of R_Σ, it is enough to check that all the elements that generates R_Σ as a ring belong to $\overline{\Sigma}$.

By construction of R_Σ (cf. page 120), we know that it is generated by the elements of R and by all the entries of matrices $\lambda(A)^{-1}$, $A \in \Sigma$; but by the way λ was constructed, $\lambda(R) = R$, so, $R \subseteq \overline{\Sigma}$. Finally, the set of all entries of matrices $\lambda(A)^{-1}$, $A \in \Sigma$ belong to $\overline{\Sigma}$ by definition of Σ–rational closure of R in R_Σ under λ (cf. page 123). ∎

Corollary III.2.4 *Let R be a ring and an let K be an epic R–field with canonical homomorphism $\mu_K: R \longrightarrow K$. Let Σ be the multiplicative set of all square matrices over R invertible over K under μ_K. Consider the universal Σ–inverting ring R_Σ with universal Σ inverting homomorphism $\lambda: R \longrightarrow R_\Sigma$. Let $\overline{\Sigma}$ be the Σ–rational closure of R in R_Σ under λ. Then, $\overline{\Sigma} = R_\Sigma$.*

Proof. This is a particular case of lemma III.2.3. ∎

Now, we present the construction of epic R–fields from singular kernels. Let K be an epic R–field, $\mu_K : R \longrightarrow K$ the canonical homomorphism and $\mathcal{P}$ the singular kernel. Let Σ be the complement of $\mathcal{P}$ in the set of all square matrices over R (so Σ is the set of all square matrices over R invertible over K; hence, in particular, Σ is multiplicative and μ_K is Σ–inverting), and recall that by $R_\mathcal{P}$ we just mean the universal Σ–inverting ring R_Σ. Let $\lambda: R \longrightarrow R_\mathcal{P}$ $(= R_\Sigma)$ be the universal Σ–inverting homomorphism. Then, we can factor μ_K by λ, i.e. from the universal property of $R_\mathcal{P}$, there is a unique ring homomorphism $\tilde{\mu}_k: R_\mathcal{P} \longrightarrow K$ such that the following triangle commutes.



We claim that $R_{\mathcal{P}}$ is a local ring with residue class field K. This will follow if we show that every element not in $ker\ \tilde{\mu}_K$ is invertible, for then, $ker\ \tilde{\mu}_K$ will be the unique maximal ideal of $R_{\mathcal{P}}$ and its residue class field is a subfield of K containing the image of R, hence equal to K, because K was an *epic* R–field. **This justifies why we singled out the subcategory of *epic* R–fields from the bigger category of R–fields**, since the former category can not be described by singular kernels.

By corollary III.2.4, we have that the Σ–rational closure of R in R_Σ is equal to R_Σ and, then, by theorem III.2.1 we know that every element of R_Σ is a component of the solution vector u of a matrix equation of the form $\lambda(A)\,u+a=0$ where $A \in \Sigma$.

We now show that every element not in $ker\ \tilde{\mu}_K$ is invertible. Let

$$u_i \in R_{\mathcal{P}} = R_\Sigma$$

be a component of the solution vector u of a matrix equation $\lambda(A)\,u + a = 0$, where A is a square matrix over R which becomes invertible over K, and define A_i as in Cramer's rule, i.e. let A_i be the matrix obtained by replacing the i–th column of A by a. If $\tilde{\mu}_K(u_i) \neq 0$, then $\tilde{\mu}_K(u_i)$ is invertible, hence $\tilde{\mu}_K \circ \lambda(A_i) = \mu_K(A_i)$ is invertible by Cramer's rule, but this means that $A_i \notin \mathcal{P}$ (to make this last claim true is the reason why we set Σ to be the set of **all** inverted matrices over K), so $\lambda(A_i)$ is invertible over $R_{\mathcal{P}}$ and so, again by Cramer's rule, u_i is a unit in $R_{\mathcal{P}}$, as claimed. ∎

Conversely, if Σ is a set of square matrices over R such that the universal

Σ–inverting ring R_Σ is a local ring, then its residue–class field is an epic R–field. Indeed, let Σ be such that R_Σ is a local ring, with residue class field K, say. By composing the natural maps we get a homomorphism $R \xrightarrow{\lambda} R_\Sigma \xrightarrow{\pi} K$, and here K is a field and an R–ring, so it is an R–field. We now show that it is epic. Let K' be the least subfield generated by the image of R in K. Any matrix A in Σ maps to an invertible matrix A_1, say, in K (because, λ maps A to an invertible matrix in R_Σ by definition of universal Σ–inverting homomorphism and, in general, any homomorphic image of an invertible matrix is invertible, so π maps $\lambda(A)$ to an invertible matrix A_1); this matrix A_1 is a non–zero divisor over K' and hence, being K' a field, A_1 has an inverse in K'. Thus, K' contains inverses of all matrices in Σ and hence contains a generating set of K, so $K = K'$, i.e. K is an epic R–field. ∎

III.3 The equivalence of epic R–fields and specializations with singular kernels and inclusions

The final come out of the discussion in the last part of the previous section is that there is a bijection between epic R–fields and their singular kernels. So, every epic R–field K has the form K_Σ, say, of a residue class field with respect to the local ring R_Σ where Σ is the multiplicative set of all matrices over R inverted over K by the canonical homomorphism μ_K.

In this section we shall show that there is a specialization between two epic R–fields iff there is an inclusion relation between their singular kernels. Since we already know that between two epic R–fields there is at most one specialization (cf. lemma III.1.1 page 116), then, it will follow that the category of epic R–fields and specializations is equivalent to the category whose objects are singular kernels of epic R–fields with inclusion mappings as morphisms.

Theorem III.3.1 *Let R be any ring, K_1, K_2 any epic R–fields, Σ_i the set of all matrices over R inverted in K_i and R_i the universal localization R_{Σ_i}, with*

maximal ideal $\mathfrak{m}_i$ *(*$i = 1, 2$*). Then the following are equivalent:*

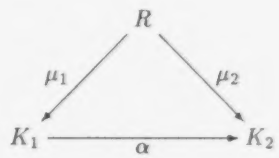
(a) there is a specialization $\alpha\colon K_1 \longrightarrow K_2$,

(b) $\Sigma_1 \supseteq \Sigma_2$,

(c) there is an R*-ring homomorphism* $f\colon R_2 \longrightarrow R_1$.

If there is a specialization from K_1 *to* K_2 *and one from* K_2 *to* K_1*, then* $K_1 \cong K_2$ *as fields.*

Proof. (a) only if (b). Let $\mu_i\colon R \longrightarrow K_i$ be the canonical homomorphism. Take $A \in \Sigma_2$, then $\mu_2(A)$ has an inverse in $\mathcal{M}(K_2)$ which is the image under α of a matrix B, say, over K_1 (recall that a local homomorphism to an epic field is surjective, cf. page 115).



Since $\alpha \circ \mu_1 = \mu_2$, then[2], $\mu_2(A)\alpha(B) = I$, so $\alpha \circ \mu_1(A)\alpha(B) = I$, hence

$$\mu_1(A)B = I + C, \text{ where } \alpha(C) = 0. \tag{III.9}$$

Thus, $C \in \mathcal{M}(ker\ \alpha)$, but $ker\ \alpha$ is the Jacobson radical of the domain of α, since the domain of α is a local R-subring of K_1 with maximal ideal $ker\ \alpha$. But since[3] for any ring R, $\mathcal{M}_n(J(R)) \subseteq J(\mathcal{M}_n(R))$ (actually they are equal, cf., for instance, Hungerford [Hun89], page 433) C belongs to the Jacobson radical of the ring of matrices over the domain of α, hence $I + C$ has an inverse (recall that an element c is in the Jacobson radical of a ring iff $1 - xcy$ has an inverse

[2]We denote by I the identity matrix over the corresponding ring and of the corresponding dimension respect to the context.

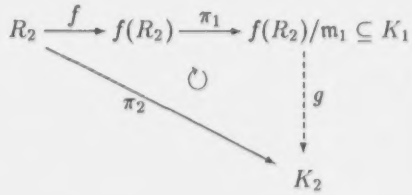
[3]Given a ring R, $J(R)$ denotes the Jacobson radical of R; if the ring is clear from the context, we simply write J for its Jacobson radical.

for every x, y in the ring; cf. Hungerford, loc. cit.). Hence, from (III.9) and the fact that B is invertible (B is a matrix over a field K_1 which has an invertible image under α, hence B must be invertible, as well), it follows that $\mu_1(A)$ is invertible, i.e. $A \in \Sigma_1$.

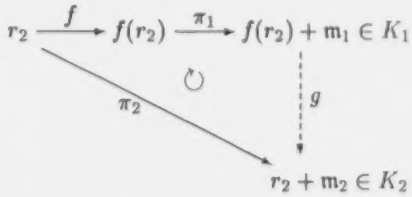
(b) only if (c). It is clear, for when (b) holds, then $\lambda_1 : R \longrightarrow R_1$, the universal Σ_1 inverting homomorphism, is Σ_2–inverting and so may be factored by λ_2.

(c) only if (a). Let $\pi_i : R_i \longrightarrow K_i$ be the natural homomorphism, i.e. $r_i \mapsto r_i + \mathfrak{m}_i$ (recall from the previous section that $K_i \cong R_i/\mathfrak{m}_i$). Then, the natural homomorphism $R_1 \xrightarrow{\pi_1} K_1$ maps $f(R_2)$ onto $f(R_2)/\mathfrak{m}_1$. Note that the R–subring $f(R_2)$ of R_1 is a local ring, since it is a homomorphic image of the local ring R_2. In terms, the R–subring $f(R_2)/\mathfrak{m}_1$ of K_1 is local, as well.

Since $\mathfrak{m}_1$ is maximal in R_1, it is a proper ideal, so it is possible to complete the following to a commutative diagram:



indeed, we check that such a g (our candidate for a local homomorphism which will give us the[4] specialization from K_1 to K_2) is well defined, since to check that it is a homomorphism is routine. So, let $g : f(R_2)/\mathfrak{m}_1 \longrightarrow K_2$ be defined by



[4]Recall that between any two epic R–fields can be at most one specialization, cf. lemma III.1.1, page 116.

$f(r_2) + \mathfrak{m}_1 \mapsto r_2 + \mathfrak{m}_2$ ($r_2 \in R_2$). Assume $f(r_2) + \mathfrak{m}_1 = f(s_2) + \mathfrak{m}_1$ where $r_2, s_2 \in R_2$. We have to show $r_2 + \mathfrak{m}_2 = s_2 + \mathfrak{m}_2$. But this holds since $f(r_2) - f(s_2) = f(r_2 - s_2) \in \mathfrak{m}_1$, so $r_2 - s_2$ must belong to $\mathfrak{m}_2$, because if that is not the case, $r_2 - s_2$ would be a unit in R_2 (recall that R_2 is a local ring with maximal ideal $\mathfrak{m}_2$), and, hence $f(r_2 - s_2)$ would be a unit in R_1 (all our homomorphism sends 1 to 1), contradicting the fact that $\mathfrak{m}_1$ is a proper ideal of R_1. Lastly, we note that g gives us the specialization from $K_1 \longrightarrow K_2$; indeed, we just verify that g is a local homomorphism. We already know that $f(R_2)/\mathfrak{m}_1$ is a local R–subring of K_1. So, we need to check that it sends non–units to non–units. But any $x \in f(R_2)/\mathfrak{m}_1$ which maps to a non–zero element of K_2 must come from an invertible element of R_2, r_2 say, (this last claim follows from the commutativity of the above diagram, indeed, if r_2 would not be invertible, then $\pi_2(r_2) = 0$, and then $g(x) = 0$, contradiction), and hence x itself must be invertible.

The last sentence follows from (b) and the bijection between epic R–fields and singular kernels of the previous section. ∎

From the above theorem III.3.1 we immediately obtain conditions for a universal field to exist:

Corollary III.3.2 *A ring R has a universal R–field iff the collection of singular kernels of epic R–fields has a greatest element (in the sense of inclusion).* ∎

III.4 Matrix ideals

We come now again to the problem of constructing epic R–fields when they exist. We already know that they will be of the form $R_\Sigma/\mathfrak{m}_\Sigma$ for some set Σ of square matrices over R that become invertible under some homomorphism into an epic R–field; our main problem in this section is to put the appropriate conditions over Σ, but actually, for technical reasons, it will be easier to characterize their complements (in the set of all square matrices over R), the singular kernels, that means a set of square matrices over R which become singular under some

homomorphism into an epic R–field, i.e. we want to characterize the singular kernels axiomatically. In the commutative case, the singular matrices are the matrices A such that *det* A (its determinant) lies in certain prime ideal, but in the general case, we do not have a determinant function, so we have to define the ideal operations (or something analogous) directly for matrices. We shall see that singular kernels show a close analogy to ideals in commutative rings, but instead of product and sum, over R, we have to define two operations on matrices over R: the diagonal sum (the analogous of the product in commutative ideal theory) and the determinantal sum (the analogous of the sum in commutative ideal theory). Also, we shall define the analogous of 0 in the commutative case, i.e., the matrices that become singular under *any* homomorphism into an epic R–field, these will be the non–full matrices.

Multiplication: as the product of two square matrices A, B (over any ring R) we take their **diagonal sum** $A \dot{+} B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. Note that over a field $A \dot{+} B$ is singular if and only if either A or B is.

Addition: it is more complicated, just as the addition of determinants is not straightforward, and in fact the latter provides the clue. Let A, B be two matrices which agree in all entries except possibly, say, in the first column: $A = (a_1, a_2, \ldots, a_n)$, $B = (a_1', a_2, \ldots, a_n)$, then the **determinantal sum** of A and B is defined as the matrix

$$A \bigtriangledown B := (a_1 + a_1', a_2, \ldots, a_n).$$

Similarly, one defines determinantal sums with respect to another column or with respect to a row. Of course it must be keep in mind that determinantal sum need not be defined. As notation, we shall always use $A \bigtriangledown B$, indicating in words the relevant column or row, when this is necessary to prevent confusion.

We observe that over a commutative ring, where determinants are defined, one has *det* $(A \bigtriangledown B) =$ *det* $A +$ *det* B, whenever the determinantal sum (for any

row or column) is defined. On the other hand, over a skew field, if A, B are singular, then so is C, as is easily seen. Further, any ring homomorphism preserves determinantal sums, therefore, if A and B both map to singular matrices under a homomorphism into a field, then so does C.

Repeated determinantal sums need to be used with care, since the operation is not everywhere defined and a fortiori not associative. Thus to say that C is a determinantal sum of matrices $A_1, \ldots, A_r$ means that we can replace any two of $A_1, \ldots, A_r$ by their determinantal sum (with respect to some row or column) and repeat this process on two matrices in the resulting set, and so on until we are left with only one matrix, namely C.

We shall now define the analogous of 0. To motivate the definition, take an integral domain R that is neither left or right Ore. This means that there exist $a, b, c, d \neq 0$ in R such that $Ra \cap Rb = 0$, $cR \cap dR = 0$. It follows easily that the matrix

$$A = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$$

is a non–zero divisor in $\mathcal{M}_2(R)$. But its image in any field has rank less than 2 and so cannot have an inverse. This suggests the following definition.

A matrix A over a ring R is said to be a **full matrix** if it is square, say $n \times n$, and not of the form $A = PQ$, where P is $n \times r$, Q is $r \times n$ and $r < n$. A matrix A over a ring R is said to be a **non–full matrix** if it is not full, i.e. it is of the form $A = PQ$, where P is $n \times r$, Q is $r \times n$ and $r < n$.

This definition is taken to mean for $n = 1$, that $a \in R$ is full if it is $\neq 0$. thus any non–zero ring with zero–divisors provides us with examples of full zero–divisors. Furthermore, for $n > 1$, take the ring $k[x, y, z, t]/(xt - yz)$ (where k is a commutative field), then the matrix $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ has zero determinant and so is a zero–divisor, but it is full. ∎

Let R be any ring. We define a **matrix pre–ideal** in R as a set $\mathcal{P}$ of square matrices over R satisfying the following three conditions:

1. P includes all non–full matrices,

2. if A, $B \in \mathcal{P}$ and their determinantal sum C (with respect to some row or column) exists, then $C \in P$,

3. if $A \in \mathcal{P}$, then $A \dot{+} B \in \mathcal{P}$ for all square matrices B.

If further, we have

4. if $A \dot{+} 1 \in \mathcal{P}$ then $A \in \mathcal{P}$,

we call $\mathcal{P}$ a **matrix ideal**. A matrix pre–ideal is said to be **proper** if it does not contain the unit matrix of any size; clearly a matrix ideal is proper precisely when it does not contain the element 1.

We note the following simple consequences from the definitions. Let $\mathcal{P}$ be any matrix pre–ideal. Then,

(a) Any square matrix with a zero row or column lies in $\mathcal{P}$. For if $A = (0A')$, where 0 is a zero column and A' is an $n \times (n-1)$ matrix, then $A = A'(0I)$, where I is the identity matrix of order $n-1$, and this shows that A is not full. Similarly for other columns or for rows.

(b) Let $A \in \mathcal{P}$, then the result of adding any right multiple of one column of A (or any left multiple of a row) to another again lies in $\mathcal{P}$.

Write $A = (a_1, a_2, ldots, a_n)$, then

$$(a_1 + a_2 c, a_2, \ldots, a_n) = A \bigtriangledown (a_2, \ldots, a_n) \begin{pmatrix} c & 0 \\ 0 & I_{n-1} \end{pmatrix};$$

on the right we have the determinantal sum with respect to the first column) of A and a non–full matrix, hence the result lies in $\mathcal{P}$ by 1. and 2..

(c) Let $A \in \mathcal{P}$, then the result of interchanging any two columns (or rows) of A and changing the sign of one of them again lies in $\mathcal{P}$.

This follows in familiar fashion from (b). Writting only the two columns in question, we have, by repeated application of (b),

$$(a_1, a_2) \longrightarrow (a_1 + a_2, a_2) \longrightarrow (a_1 + a_2, -a_1) \longrightarrow (a_1, -a_1)$$

.

(d) Let A, B be any square matrices, say of orders m, n respectively. Then for any $n \times m$ matrix C,

$$\text{(III.10)} \qquad \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in \mathcal{P} \text{ iff } \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \mathcal{P}.$$

For given A, B, C, let a_1, c_1 be the first columns of A, C respectively, and write $A = (a_1 A')$, $C = (c_1 C')$, then

$$\text{(III.11)} \qquad \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = \begin{pmatrix} a_1 & A' & 0 \\ 0 & C' & B \end{pmatrix} \nabla \begin{pmatrix} 0 & A' & 0 \\ c_1 & C' & B \end{pmatrix},$$

where the determinantal sum is with respect to the first column. We have

$$\begin{pmatrix} 0 & A' & 0 \\ c_1 & C' & B \end{pmatrix} = \begin{pmatrix} A' & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} 0 & I & 0 \\ c_1 & C' & B \end{pmatrix};$$

thus the second matrix on the right of (III.11) is not full and so lies in $\mathcal{P}$. Now (III.11) may be rewritten

$$\begin{pmatrix} a_1 & A' & 0 \\ 0 & C' & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \begin{pmatrix} 0 & A' & 0 \\ -c_1 & C' & B \end{pmatrix},$$

where the second matrix on the right is again non–full. Hence

$$\begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in \mathcal{P} \text{ iff } \begin{pmatrix} a_1 & A' & 0 \\ 0 & C' & B \end{pmatrix} \in \mathcal{P}.$$

In a similar way we can vary the other columns of C, and so prove the assertion. An entirely analogous argument, using rows, shows that for any $m \times n$ matrix C,

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \in \mathcal{P} \text{ iff } \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \mathcal{P}.$$

(e) If $\mathcal{P}$ is actually a matrix ideal, then for any two square matrices A, B of the same size, $AB \in \mathcal{P}$, say. Then $A \dot{+} B \in \mathcal{P}$ by (III.11); using (d) and (b) several times, we obtain in turn

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \to \begin{pmatrix} A & 0 \\ I & B \end{pmatrix} \to \begin{pmatrix} 0 & -AB \\ I & B \end{pmatrix} \to \begin{pmatrix} AB & 0 \\ -B & I \end{pmatrix} \to \begin{pmatrix} AB & 0 \\ 0 & I \end{pmatrix}.$$

Now, an application of 4. shows that $AB \in \mathcal{P}$.

(f) If A belongs to a matrix ideal $\mathcal{P}$, then the result of permuting the rows or columns of A in any way again belongs to $\mathcal{P}$. For we can permute the rows (or columns) by (c) and use (e) to get rid of the minus signs.

(g) A matrix ideal $\mathcal{P}$ is proper iff some square matrix does not belong to $\mathcal{P}$. Indeed, if $\mathcal{P}$ is proper, then $1 \notin \mathcal{P}$, by definition. Conversely, if $\mathcal{P}$ is improper, then $I \in \mathcal{P}$ and hence by (e), $A = AI \in \mathcal{P}$, for any square matrix A.

Let $(\mathcal{P}_\lambda)$ be any family of matrix ideals, then it is clear that $\mathcal{P} := \bigcap \mathcal{P}_\lambda$ is again a matrix ideal. We can therefore speak of the **"least" matrix ideal containing a given set $\mathcal{X}$** of square matrices, namely the intersection of all matrix ideals containing $\mathcal{X}$. This least matrix ideal containing $\mathcal{X}$ is also called the **matrix ideal generated by $\mathcal{X}$**. Similarly, we can define the **matrix pre–ideal generated by $\mathcal{X}$**. Explicitly, this is obtained by forming the determinantal

sum of matrices $X \dot{+} A$ ($X \in \mathcal{X}$, A any square matrix) and of non–full matrices. For this set is contained in any matrix pre–ideal containing $\mathcal{X}$, and it satisfies 1. and 2.; let us show that it also satisfies 3.. If the set contains C, the (for suitable bracketing),

$$C = B_1 \bigtriangledown \cdots \bigtriangledown B_r \qquad (B_i = X \dot{+} A \text{ or non–full}), \tag{III.12}$$

hence for any square matrix P,

$$C \dot{+} P = (B_1 \dot{+} P) \bigtriangledown \cdots \bigtriangledown (B_r \dot{+} P),$$

with the same bracketing.

Thus the matrix pre–ideal generated by a set $\mathcal{X}$ consists precisely of all determinantal sums C of the form (III.12). Now the connection between matrix pre–ideals and matrix ideals is given by

Proposition III.4.1 *Let $\mathcal{P}$ be any matrix pre–ideal, then the least matrix ideal containing $\mathcal{P}$ is given by*

$$\overline{\mathcal{P}} = \{A : \ A \dot{+} I \in \mathcal{P} \text{ for some unit–matrix } I\}. \tag{III.13}$$

Proof. If $\overline{\mathcal{P}}$ is defined by (III.13), then $\overline{\mathcal{P}} \supseteq \mathcal{P}$ and any matrix ideal containing $\mathcal{P}$ must also contain $\overline{\mathcal{P}}$, so it only remains to show that $\overline{\mathcal{P}}$ is itself a matrix ideal. Properties 1.–3. are clear. If $A \dot{+} 1 \in \overline{\mathcal{P}}$ then $A \dot{+} 1 \dot{+} I \in \mathcal{P}$, i.e. $A \dot{+} I \in \mathcal{P}$ (for a unit matrix of larger order than before), and hence $A \in \overline{\mathcal{P}}$. Thus, 4. also holds, and the result follows. ∎

Corollary III.4.2 *A matrix pre–ideal generates a proper matrix ideal iff it is itself proper. More specifically, the matrix ideal generated by a set $\mathcal{X}$ is proper iff the unit matrix I (of any size) can not be expressed as a determinantal sum of non–full matrices and matrices of the form $X \dot{+} A$, where $X \in \mathcal{X}$ and A is any square matrix.* ∎

Let $\mathcal{L}$ be the matrix pre–ideal generated by the empty set. Clearly this is the least matrix pre–ideal, and it consists precisely of all determinantal sums of non–full matrices. By the last corollary we find

Proposition III.4.3 *Let R be any ring, then R has proper matrix ideals iff no unit–matrix can be written as a determinantal sum of non–full matrices.* ∎

III.5 Prime matrix ideals and their characterization as singular kernels

In the study of homomorphisms of commutative rings into fields prime ideals play an important role, and we shall find that in the general case there is an analogue in the prime matrix ideals, now to be defined. It will be convenient to begin by defining a multiplication of matrix ideals; this is an associative and commutative operation, like the multiplication of ideals in commutative rings.

Given two matrix ideals $\mathcal{P}_1, \mathcal{P}_2$ in a ring R, their **product**, denoted by $\mathcal{P}_1\mathcal{P}_2$, is defined as the matrix ideal generated by all $A_1 \dotplus A_2$ with $A_i \in \mathcal{P}_i$ $(i = 1, 2)$.

The product so defined is easily seen to be associative. We write $\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$ etc. for repeated products, and abbreviate $\mathcal{P}\mathcal{P}$, $\mathcal{P}\mathcal{P}\mathcal{P}$, ... as $\mathcal{P}^2$, $\mathcal{P}^3$, ... From property (f), of the previous section, it follows that the product is commutative, and by 3., in the definition of matrix pre–ideal (see previous section), it is contained in the intersection of the factors:

$$\mathcal{P}_1\mathcal{P}_2 = \mathcal{P}_2\mathcal{P}_1 \subseteq \mathcal{P}_1 \cap \mathcal{P}_2.$$

The following lemma is often useful in constructing products:

Lemma III.5.1 *Let $\mathcal{X}_1$, $\mathcal{X}_2$ be any sets of square matrices, $\mathcal{X}$ the set of matrices $A_1 \dotplus A_2$ $(A_i \in \mathcal{X}_i)$, and $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}$ the matrix ideals generated by $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{X}$ respectively, then $\mathcal{P} = \mathcal{P}_1\mathcal{P}_2$.*

Proof. Clearly $\mathcal{X} \subseteq \mathcal{P}_1\mathcal{P}_2$, hence $\mathcal{P} \subseteq \mathcal{P}_1\mathcal{P}_2$; to establish equality it is enough to show that $A_1 \dot{+} A_2 \in \mathcal{P}$ for any $A_i \in \mathcal{P}_i$. Take $A_i \in \mathcal{P}_i$, then $A_1 \dot{+} I$ is a determinantal sum of matrices B_μ which are either non–full or diagonal sums with a term in $\mathcal{X}_1$; similarly $A_2 \dot{+} I$ is a determinantal sum of matrices C_ν which are either non–full or diagonal sums with a term in $\mathcal{X}_2$. Therefore $A_1 \dot{+} A_2 \dot{+} I$ is a determinantal sum of the matrices $B_\mu \dot{+} C_\nu$ which are either non–full or a diagonal sum with a term in $\mathcal{X}$. Hence $A_1 \dot{+} A_2 \in \mathcal{P}$, and it follows that $\mathcal{P} = \mathcal{P}_1\mathcal{P}_2$ as asserted. ∎

A matrix ideal $\mathcal{P}$ is said to be **prime** if it is proper and

$$\text{if } A \dot{+} B \in \mathcal{P} \text{ then } A \in \mathcal{P} \text{ or } B \in \mathcal{P}.$$

A matrix ideal $\mathcal{P}$ is said to be **semiprime**

$$\text{if } A \dot{+} A \in \mathcal{P} \text{ then } A \in \mathcal{P}.$$

An alternative description of these notions is given in

Proposition III.5.2 *Let $\mathcal{P}$ be a matrix ideal in a ring R; then*

(i) $\mathcal{P}$ is prime iff $\mathcal{P}$ is proper and for any matrix ideals $\mathcal{P}_1$, $\mathcal{P}_2$ we have: if $\mathcal{P}_1\mathcal{P}_2 \subseteq \mathcal{P}$ then $\mathcal{P}_1 \subseteq \mathcal{P}$ or $\mathcal{P}_2 \subseteq \mathcal{P}$,

(ii) $\mathcal{P}$ is semiprime iff for any matrix ideal $\mathcal{L}$, if $\mathcal{L}^2 \subseteq \mathcal{P}$ then $\mathcal{L} \subseteq \mathcal{P}$.

Proof. (i) Let $\mathcal{P}$ be prime and $\mathcal{P}_1\mathcal{P}_2 \subseteq \mathcal{P}$ but $\mathcal{P}_i \not\subseteq \mathcal{P}$ $(i = 1, 2)$. Then there exists $A_i \in \mathcal{P}_i$ but $A_i \notin \mathcal{P}$. Since $\mathcal{P}$ is prime, $A_1 \dot{+} A_2 \notin \mathcal{P}$, but $A_1 \dot{+} A_2 \in \mathcal{P}_1\mathcal{P}_2 \subseteq \mathcal{P}$, a contradiction.

Conversely, assume that $\mathcal{P}$ satisfies the given conditions, and let $A_1 \dot{+} A_2 \in \mathcal{P}$. Write (A_i) for the matrix ideal generated by A_i, then by lemma III.5.1, the product $(A_1)(A_2)$ is generated by $A_1 \dot{+} A_2$, and hence $(A_1)(A_2) \subseteq \mathcal{P}$. Therefore $(A_i) \subseteq \mathcal{P}$ for $i = 1$ or 2, say $i = 1$, and so $A_1 \in \mathcal{P}$, showing that $\mathcal{P}$ is prime.

(ii) Similarly if $\mathcal{P}$ is semiprime and $\mathcal{L}^2 \subseteq \mathcal{P}$, let $A \in \mathcal{L}$, then $A \dotplus A \in \mathcal{L}^2 \subseteq \mathcal{P}$, hence $A \in \mathcal{P}$, and so $\mathcal{L} \subseteq \mathcal{P}$, as claimed. Conversely, if $\mathcal{P}$ satisfies the given condition, and $A \dotplus A \in \mathcal{P}$, then $(A)^2$ is generated by $A \dotplus A$ and so $(A)^2 \subseteq \mathcal{P}$, hence $(A) \subseteq \mathcal{P}$, whence $A \in \mathcal{P}$. This shows that $\mathcal{P}$ is semiprime. ∎

By $\dotplus^r A$ we mean the diagonal sum of A with itself r times, where A is a square matrix over a ring A and $r \in \mathbb{N}$. Let $\mathcal{P}$ be any matrix ideal and define its **radical** as the set

$$\sqrt{\mathcal{P}} = \{A : \dotplus^r A \in \mathcal{P} \text{ for some } r \in \mathbb{N}\}.$$

Clearly $\sqrt{\mathcal{P}} \supseteq \mathcal{P}$; we assert that $\sqrt{\mathcal{P}}$ is the least semiprime matrix ideal containing $\mathcal{P}$. In the first place, any semiprime matrix ideal containing $\mathcal{P}$ must contain $\sqrt{\mathcal{P}}$ for if $A \in \sqrt{\mathcal{P}}$, then $\dotplus^r A \in \mathcal{P}$ for some r; hence this holds for any $r' \geq r$, and taking $r' = 2^k$, we have that $\dotplus^{2^k} A \in \mathcal{P}$. Now it follows (by induction on k) that any semiprime matrix ideal containing $\mathcal{P}$ also contains A, and hence contains $\sqrt{\mathcal{P}}$. Thus if we can show that $\sqrt{\mathcal{P}}$ is a semiprime matrix ideal we shall have shown that it is the least semiprime containing $\mathcal{P}$. Properties 1., 2., 4. clearly hold; to prove 3. we note that $\dotplus^n(A \bigtriangledown B)$ is a determinantal sum of terms $C_1 \dotplus \cdots \dotplus C_n$ where each C_i is A or B. Hence if $\dotplus^r A$ and $\dotplus^s B$ lie in $\mathcal{P}$, then $\dotplus^{r+s-1}(A \bigtriangledown B) \in \mathcal{P}$; therefore $\sqrt{\mathcal{P}}$ also satisfies 3. and so is a matrix ideal. If $A \dotplus A \in \sqrt{\mathcal{P}}$, say $\dotplus^{2r} A \in \mathcal{P}$, then $A \in \sqrt{\mathcal{P}}$, so $\sqrt{\mathcal{P}}$ is semiprime, as claimed. ∎

To relate semiprime and prime matrix ideals we first show that the familiar method of constructing prime ideals as maximal ideals still works for matrix ideals.

Theorem III.5.3 *In any ring R, let Σ be a non-empty set of square matrices closed under diagonal sums; then any matrix ideal $\mathcal{P}$ which is maximal disjoint from Σ is prime.*

Proof. Let $\mathcal{P}_1\mathcal{P}_2 \subseteq \mathcal{P}$ but $\mathcal{P}_i \not\subseteq \mathcal{P}$, then $\mathcal{P}_i \cap \Sigma \neq \emptyset$. Take $A_i \in \mathcal{P}_i \cap \Sigma$, then

$A_1 \dotplus A_2 \in \Sigma$, and $A_1 \dotplus A_2 \in \mathcal{P}_1\mathcal{P}_2 \subseteq \mathcal{P}$, which is a contradiction. So we have $\mathcal{P}_i \subseteq \mathcal{P}$ for $i = 1$ or 2. Moreover, $\mathcal{P}$ is proper because $\Sigma \neq \emptyset$; this shows that $\mathcal{P}$ is prime. ∎

Whether maximal matrix ideals as in theorem III.5.3 exist or not, depends on whether there are any proper matrix ideals in R. Thus let Σ be any non–empty set of square matrices closed under diagonal sums, then any matrix ideal disjoint from Σ must be proper. If there is one, i.e. if Σ is disjoint from the least matrix ideal, then the collection $\mathcal{C}$ of all matrix ideals disjoint from Σ is non–empty. Clearly $\mathcal{C}$ is inductive, and hence there are maximal matrix ideals disjoint from Σ, to which the theorem can be applied.

The connection between semiprime and prime matrix ideals is given in

Theorem III.5.4 *In any ring R, a matrix ideal is semiprime iff it is an intersection of prime matrix ideals.*

Proof. Let $\mathcal{P} = \bigcap \mathcal{P}_\lambda$, where $\mathcal{P}_\lambda$ is prime. If $A \dotplus A \in \mathcal{P}$, then $A \dotplus A \in \mathcal{P}_\lambda$ for all λ, hence $A \in \mathcal{P}_\lambda$ for all λ, so $A \in \mathcal{P}$ and $\mathcal{P}$ is semiprime.

Conversely, let $\mathcal{P}$ be semiprime. It will be enough to find, for each $A \notin \mathcal{P}$, a prime matrix ideal $\mathcal{P}_A$ containing $\mathcal{P}$ but not A, for then

$$\mathcal{P} = \bigcap \{\mathcal{P}_A : \ A \notin \mathcal{P}\}.$$

Let $A \notin \mathcal{P}$ be given and consider the set Σ_A of all diagonal sums of copies of A. Since $\mathcal{P}$ is semiprime, $\Sigma_A \cap \mathcal{P} = \emptyset$, and clearly Σ_A is non–empty and closed under diagonal sums. Hence there is a maximal matrix ideal $\mathcal{P}_A$ containing $\mathcal{P}$ and disjoint from Σ_A. By theorem III.5.3, $\mathcal{P}_A$ is prime and $A \notin \mathcal{P}_A$. Hence $\bigcap \mathcal{P}_A = \mathcal{P}$, and the result follows. ∎

Let R be any ring with a prime matrix ideal $\mathcal{P}$, and denote by Σ the complement of $\mathcal{P}$ (in the set of all square matrices). We would like that R_Σ be a local ring; this will follow once we know that $R_\Sigma \neq 0$. In fact we shall see that

there is an R–field K in which the set of singular matrices is precisely $\mathcal{P}$. From the construction of epic R–fields from their singular kernels (cf. page 128), it then follows that R_Σ is a local ring with residue–class field K.

We can now state the main result of this section. It will be presented without proof because this is long (and can be found in Cohn's book [Coh85], chapter 7); more over a knowledge of the proofs is not necessary to apply the results as we shall do in the next section.

Theorem III.5.5 *Let R be any ring and $\mathcal{P}$ a prime matrix ideal in R. Then there exists an R–field K such that $\mathcal{P}$ is the precise class of matrices mapped to singular matrices under the canonical homomorphism $R \longrightarrow K$.* ∎

Taken in conjunction with theorem III.3.1 (on page 130), this result shows that the category of R–fields and specializations is equivalent to the category of prime matrix ideals and inclusions, in precise analogy with the prime ideals in a commutative ring. For example, R has a universal R–field iff there is a unique least prime matrix ideal (cf. corollary III.3.2 on page 133).

III.6 General criterion for a ring to be embeddable and to have a universal field of fractions

Of course, a ring need not have any prime matrix ideals at all (see introduction to chapter III); to find if it has any we go back to the method of generating matrix ideals described in section III.4. In any ring R, denote by $\mathcal{L}$ the set of all determinantal sums of non–full matrices. Thus $A \in \mathcal{L}$ iff

$$A = C_1 \bigtriangledown \cdots \bigtriangledown C_t,$$

where each C_i is non–full and the right–hand side is suitable bracketed. Clearly $\mathcal{L}$ is the least matrix pre–ideal in R (cf. section III.4). Let $\overline{\mathcal{L}}$ be the matrix ideal generated by $\mathcal{L}$ and put $\mathcal{N} = \sqrt{\overline{\mathcal{L}}}$, then $\mathcal{N}$ is proper iff $\mathcal{L}$ is proper. By theorem III.5.4 on page 143, $\mathcal{N}$ is the intersection of all prime matrix ideals, so $\mathcal{N}$ is proper iff R has prime matrix ideals. But the latter correspond to homomorphisms into fields, so we find that $\mathcal{N}$ is proper iff R has a homomorphism into a field. We therefore obtain the following criterion for the existence of field homomorphisms:

Theorem III.6.1 *Let R be any ring. Then there exists a homomorphism of R into a field iff no unit matrix in R can be written as a determinantal sum of non–full matrices.* ∎

We also obtain a criterion for the invertibility of matrices:

Theorem III.6.2 *Let R be a ring and A any square matrix over R. Then*

(i) there is a homomorphism of R into a field mapping A to an invertible matrix iff no diagonal sum $I \dotplus^r A$ can be written as a determinantal sum of non–full matrices,

(ii) there is a homomorphism of R into a field mapping A to a singular matrix iff no unit matrix I can be written as a determinantal sum of non–full matrices and matrices of the form $A \dotplus B$ (where B is any square matrix).

Proof. Both parts will follow if we prove that for any matrices P, Q there is a homomorphism to a field mappings P to an invertible matrix and Q to a singular matrix iff no diagonal sum $I \dotplus^r P$ can be written as a determinantal sum of non–full matrices and matrices $Q \dotplus B$ (where B is any square matrix). For (i) we take $P = A$, $Q = 0$, and for (ii) we take $P = I$, $Q = A$.

The condition for a homomorphism of the required sort to exist is that there should be a prime matrix ideal containing Q but no P. Let (Q) be the matrix ideal generated by Q, then there is a prime matrix ideal containing Q but not

P iff $P \notin \sqrt{(Q)}$. So the required condition is that $\dot{+}^r P \notin (Q)$ for all r, i.e. there is no equation

(III.14) $I \dot{+}^r P = C_1 \bigtriangledown \cdots \bigtriangledown C_t$ (C_i non-full or of form $Q \dot{+} B_i$). ∎

From this theorem it is possible to obtain a criterion for the embeddability of a ring in a field.

Corollary III.6.3 *A ring R can be embedded in a field iff it is an integral domain, and no non-zero scalar matrix aI can be written as a determinantal sum of non-full matrices.*

Proof. The condition is clearly necessary from theorem III.6.2; when it holds, then there is an R-field for which aI is invertible, for each $a \neq 0$ in R. Thus R can be embedded in a product of fields and for an integral domain this means that R can be embedded in a field, cf. for instance, Cohn [Coh71b]. ∎

An alternative formulation is the following:

Corollary III.6.4 *A ring R is embeddable in a field iff no diagonal matrix with non-zero elements on the main diagonal can be written as a determinantal sum of non-full matrices.*

Proof. For if $ab = 0$, then

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 1 & b \end{pmatrix} \bigtriangledown \begin{pmatrix} 0 & 0 \\ -1 & b \end{pmatrix} = \begin{pmatrix} a \\ 1 \end{pmatrix}^{(1,,b)} \bigtriangledown \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{(-1,,b)},$$

and here both matrices on the right are non-full. Thus the condition of corollary III.6.4 is sufficient to exclude zero-divisors, and by corollary III.6.3 is therefore sufficient for embeddability in a field. The converse is clear. ∎

We have already found the condition for the existence of a universal R-field: it was that the radical of the least matrix ideal, the set $\mathcal{N}$ constructed before

theorem III.6.1, should be prime. Moreover, there will be a universal field of fractions iff, further, $\mathcal{N}$ contains no non–zero elements of R. We shall now see conditions for the existence of universal fields of fractions in which every full matrix is invertible.

Theorem III.6.5 *Let R be any ring. Then there is an R–field in which every full matrix of R can be inverted (and which is therefore a universal field of fractions) iff*

(i) the diagonal sum of any full matrices is full, and

(ii) the determinantal sum of any non–full matrices (where defined) in non–full.

Proof. For the conclusion requires that the set of non–full matrices should be the unique least prime matrix ideal. If this is to be the case, (i) and (ii) must hold. Conversely, when they are satisfied, then the non–full matrices form a matrix ideal by (ii), necessarily the least, and it is prime by (i). ∎

The conditions of theorem III.6.5 are not easy to apply; but there is just one case where they can be checked without difficulty, namely for **semifirs**, i.e. rings in which finitely generated (left or) right ideals are free of unique rank. Once the basic properties of semifirs have been derived, such verification takes less than a page (cf. Cohn [Coh85]), but since we have not developed the linear algebra for semifirs required here, we omit a detailed proof:

Theorem III.6.6 *Every semifir has a universal field of fractions, obtained as the universal ring inverting all the full matrices.* ∎

Finally, we mention that the following are semifirs:

- free algebras over a commutative field, (cf. [Coh63]),
- group algebras of free groups over a commutative field, (cf. [Coh67]),

- free products of skew fields over a common subfield, (cf. [Coh63]),

hence, they are embeddable in skew fields.

CHAPTER IV

Dubrovin's partial solution to a problem of Malcev

In this last chapter we shall quote without proof the most important result from a paper of Dubrovin [Dub94] which led to a partial solution of a famous and longstanding problem of A. I. Malcev on the embeddability of the group ring of a right ordered group (over a skew field) into a division ring. In chapter II we saw the solution of a particular case of this problem, namely when the group was left and right ordered, by means of the Malcev–Neumann constructions of formal power series.

Recall from page 52 that a group G is said to be left orderable if it can be linearly ordered in such a way that if $g_1 \leq g_2$ then $hg_1 \leq hg_2$ for any $h, g_1, g_2 \in G$.

Problem (Malcev, A. I.). Let F be a skew field and G be a left orderable group. Can the group ring FG be embedded into a skew field?.

It is well–known (cf. [Dub94]) that it is sufficient to solve Malcev's problem for the group $Aut(\mathbb{Q}, \leq)$ of all order–automorphisms of the rational numbers with their usual order. From this point of view, Dubrovin presents his partial

solution of Malcev's problem: theorem IV.8.1 says that, under certain extra conditions, FG can be embedded in a skew field in the case when G is the **universal covering group** of $SL(2,\mathbb{R})$.

The general solution to Malcev's problem remains open.

IV.1 The main idea of Dubrovin's embedding

The main idea of Dubrovin's work is as follows. Let L be the set of all formal series $\gamma = \sum k_g g$ ($g \in G$, $k_g \in F$) with well ordered support *supp* γ. If G is a linearly ordered group, then L is a skew field under the naturally defined operations of addition and multiplication, as we saw in chapter II. But if G is just a left ordered group, L will only be a left FG–module; still one may treat FG as a subring of the ring $Q = End(L_F)$. Dubrovin introduces the **rational closure** D of the ring FG in Q. The ring D is the main object of investigation through out his paper. It is also introduced the notion of **complexity** on D. For example, an element $g \in G\backslash\{1\}$ is simpler than $1+g$ which is simpler than $(1+g)^{-1}$ and so on. This relation is a refinement of the notion of **depth** of elements in a universal skew field of fractions as studied by P. M. Cohn [Coh85], chapter 7. It turns out that this complexity relation makes D a well–preordered set and thus it is possible to prove results by transfinite induction on the complexity. Starting from the group G and jumping from an element $d \in D$ to more complex elements it can be proved that all non–zero elements in D are invertible, and moreover, they possesses other nice properties such as **σ–linearity, mononotonicity, fully rationality**, etc. It is essential in order to be able to show that D is indeed a skew field to watch these additional properties.

IV.2 Automorphisms of linearly ordered sets

Through this chapter $(\Gamma, \leq)$ will be a loset (linearly ordered set), $\mathbf{A}$ will be a group and $\mathbf{V}: A \longrightarrow Aut\ \Gamma$ will be a homomorphism. If $a \in A$ and $h \in \Gamma$ we shall write $V_a(h)$ for the image of h under the automorphism $V_a: \Gamma \longrightarrow \Gamma$.

In what follows, keep in mind the construction of the real numbers from the rationales by means of Dedekind cuts. A subdivision $\Gamma = \Gamma_1 \cup \Gamma_2$ will be called a **Dedekind cut** if:

a) $h_1 < h_2$ for any $h_1 \in \Gamma_1$ and $h_2 \in \Gamma_2$;

b) if Γ_1 has not the largest element then Γ_2 is not empty and has not a smallest element.

The set of all Dedekind cuts of the loset Γ will be called the **Dedekind closure** of Γ and will be denoted as $\overline{\Gamma}$.

Let $\alpha:\ \Gamma = \Gamma_1 \cup \Gamma_2$ and $\beta:\ \Gamma = \Gamma_1' \cup \Gamma_2'$ be two Dedekind cuts. Then we shall write $\alpha \leq \beta$ or $\beta \geq \alpha$ if for every element $h \in \Gamma_1$ there exists an element $h' \in \Gamma_1'$ with $h \leq h'$. The next theorem is well known from the real numbers.

Theorem IV.2.1 *The Dedekind closure $\overline{\Gamma}$ with the relation $\leq$ defined above is a linearly ordered set. The map $\aleph: \Gamma \longrightarrow \overline{\Gamma}$ which attaches to every $h \in \Gamma$ the Dedekind cut*

$$\Gamma := \{l \in \Gamma |\ l \leq h\} \cup \{l \in \Gamma | l > h\}$$

is a monotone inclusion of $(\Gamma, \leq)$ into $(\overline{\Gamma}, \leq)$. ∎

Let us identify Γ with the image $\aleph(\Gamma)$. Thus we shall consider Γ as a subset of the loset $\overline{\Gamma}$ and for every Dedekind cut $\Gamma = \Gamma_1 \cup \Gamma_2$ there exists a unique element $\alpha \in \overline{\Gamma}$ with $h_1 \leq \alpha < h_2$ for every $h_1 \in \Gamma_1$ and $h_2 \in \Gamma_2$. It follows that every non–empty upper bounded subset S of the Dedekind closure $\overline{\Gamma}$ has a least upper bound $supS' \in \overline{\Gamma}$ and every non–empty lower bounded subset T has a lower bound $infT \in \overline{\Gamma}$.

We shall need the next simple property of a Dedekind cut.

Proposition IV.2.2 *Let $\varepsilon \in \overline{\Gamma}\backslash\Gamma$ and $\alpha, \beta \in \overline{\Gamma}$ with $\alpha < \varepsilon < \beta$. Then there exist $h_1, h_2 \in \Gamma$ such that $\alpha < h_1 < \varepsilon < h_2 < \beta$.*

Proof. Let $\Gamma_1 := \{h \in \Gamma |\ h \leq \varepsilon\}$, $\Gamma_2 := \{h \in \Gamma |\ h > \varepsilon\}$. Then, $\Gamma = \Gamma_1 \cup \Gamma_2$ is a Dedekind cut and Γ_1 has no largest element. By definition of a Dedekind closure, there exists an element $h_1 \in \Gamma_1$ with $\alpha < h_1$. Since as $\Gamma_2 \neq \emptyset$ there exists an element $h_2 \in \Gamma_2$ with $h_2 < \beta$. ∎

Let us turn to our representation $V : A \longrightarrow Aut\ \Gamma$ and take any elements $a \in A, \varepsilon \in \overline{\Gamma}\backslash\Gamma$. Then, we set

$$V_a(\varepsilon) = \lim_{\substack{h \longrightarrow \varepsilon \\ h \in \Gamma}} V_a(h). \tag{IV.1}$$

Definition (IV.1) is correct due to proposition IV.2.2, and moreover, it can be verified that $V_a : \overline{\Gamma} \longrightarrow \overline{\Gamma}$ is an automorphism.

For a given element $\varepsilon \in \overline{\Gamma}$ the notation $\mathbf{P}_\varepsilon$ will be used throughout for the set $\{a \in A | V_a(\varepsilon) \geq \varepsilon\}$ and $\mathbf{A}_\varepsilon$ will be used for the set $\{a \in A |\ V_a(\varepsilon) = \varepsilon\}$. The notation $\mathbf{U(P)}$ will be used for the set of all units of a monoid $(P, .)$.

IV.3 The universal covering group of SL(2,ℝ) and the module of formal series

We shall present the universal covering group of $SL(2,\mathbb{R})$ as a group of order-preserving bijections of the line $\mathbb{R}$. First we denote by

$$\mathbb{S} = \left\{ r(t) := \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} |\ t \in \mathbb{R} \right\},\ \mathbb{U} = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} |\ a, b \in \mathbb{R}; a > 0 \right\}.$$

Note that $\mathbb{S}$ and $\mathbb{U}$ are subgroups of $SL(2,\mathbb{R})$. It is well known that any element $g \in SL(2,\mathbb{R})$ can be uniquely written in the form $g = r(t).u$, for some $r(t) \in \mathbb{S}$

and $u \in \mathbb{U}$.

Let $\Gamma = \{x^t | \, t \in \mathbb{R}\}$ be a group with a multiplicative law of composition, $x^t.x^{t'} = x^{t+t'}$, and an an order $x^t \leq x^{t'}$ iff $t \leq t'$. The **universal covering group** $\mathbb{G}$ of the group $SL(2,\mathbb{R})$ can be described as the set of all $x^t u$ ($t \in \mathbb{R}$, $u \in \mathbb{U}$) with the law of composition

$$(x^{t_1}u_1)(x^{t_2}u_2) = x^{t_1+2\pi k+t}u \tag{IV.2}$$

where $k \in \mathbb{Z}$ is such that $0 \leq t_2 - 2\pi k < 2\pi$ and $t \in [0, 2\pi]$ is such that $r(t)u = u_1 r(t_2)u_2$ in the group $SL(2,\mathbb{R})$.

Let K be a ring, Γ a linearly ordered set and $\{M_h | \, h \in \Gamma\}$ be a set or right K–modules indexed by Γ. The set L of all power series

$$\gamma = \sum m_h, \; h \in \Gamma, \; m_h \in M_h, \tag{IV.3}$$

such that $supp\gamma = \{h \in \Gamma | \, m_h \neq 0\}$ is a well–ordered set, will be called the **module of formal series**. The set L is indeed a right K–module, if addition and multiplication is defined component–wise, which is possible, since

$$supp(\gamma_1 + \gamma_2) \subseteq supp(\gamma_1) \cup supp(\gamma_2); \quad supp(\gamma k) \subseteq supp(\gamma) \tag{IV.4}$$

for $\gamma_1, \gamma_2 \in L, \; k \in K$.

We define the norm $v(\gamma)$ of a non–zero element γ in L as the minimal element in $supp\gamma$ and set $v(0) = \infty$.

Any series of the form m, with $m \in M_h$, will be called **homogeneous**, or more precisely **h–homogeneous**. For any non–zero series γ there exists a non–zero homogeneous summand a of γ such that $v(\gamma - a) > v(\gamma)$. This summand will be denoted by $\partial\gamma$ and will be called a **homogeneous beginning** of γ.

Let $Q := EndL_K$. As usual, we shall call an element of $q \in Q$ a **projection** if $q^2 = q$, and we shall define two special types of projections of Q as follows.

Let $h \in \Gamma$ and γ be an element in L as in (IV.3). Then the homogeneous summand m_h of γ is called the **h–component** γ_h of γ. We observe that $\gamma_h \neq 0$ iff $h \in supp\gamma$. Now, let ε be an element in $(\overline{\Gamma}, \infty)$. Then, the **$\varepsilon$– beginning**, or simpler a beginning, of γ is the series $\gamma_{<\varepsilon} = \sum m'_h,\ h \in \Gamma,\ m'_h = m_h$ for $h < \varepsilon$ and $m'_h = 0$, for $h \geq \varepsilon$.

The mapping defined by $\gamma \longrightarrow \gamma_{<\varepsilon}$ will be called the **ε–cutting**. With $\beta \preceq \gamma$ we shall denote the fact that β is an ε–beginning of γ for some ε and we shall write $\beta \prec \gamma$ if $\beta \preceq \gamma$ but $\beta \neq \gamma$, and say that β is a **proper ε–beginning** of γ. The decomposition $\gamma = \beta + \gamma'$, where β is an ε–beginning of γ, will be called the **ε–cutting of γ**. If $\varepsilon \leq v(\gamma)$ then the equality $\gamma = 0 + \gamma$ will be the ε–cutting. In the other extreme, when ε is greater than any element of $supp\gamma$, we obtain that $\gamma = \gamma + 0$ is the ε–cutting.

IV.4 Summable systems and σ–linear, monotone and monomial endomorphisms of the module of formal series

Let $\{\gamma_i |\ i \in I\}$ be a family (also called system) of elements in L. We say that this family is **summable** or, equivalently, that the series $\sum \gamma_i \in I$, **converges**, if the following conditions hold:

a) $\bigcup supp\ \gamma_i,\ i \in I$, is a well–ordered set;

b) for every $h \in \Gamma$, the set $\Delta(h) := \{i \in I |\ (\gamma_i)_h \neq 0\}$ is finite.

In this case we call the series $\gamma \in L$ with $\gamma_h = \sum (\gamma_i)_h,\ i \in \Delta(h),\ h \in \Gamma$, the **sum** of the system $\{\gamma_i |\ i \in I\}$.

If $q \in Q := End_K L$ and $\gamma \in L$, then we shall denote by $q[\gamma]$ the image of γ under q. An endomorphism $q \in Q$ will be called **σ–linear** if for any summable family $\{\gamma_i |\ i \in I\}$, the family $\{q[\gamma_i] |\ i \in I\}$ is summable and

$q[\sum \gamma_i] = \sum q[\gamma_i]$, $i \in I$. An endomorphism $q \in Q$ will be called **monotone** if the inequality $v(\alpha) \leq v(\beta)$ holds for any $\alpha, \beta \in L$ iff $v(q[\alpha]) \leq v(q[\beta])$. An endomorphism $q \in Q$ is called **monomial** if for every $h \in \Gamma$ there exists $j \in \Gamma$ with $q(M_h) \subseteq M_j$.

Let A be a subset of a ring Q. The smallest subring D of the ring Q which contains A and is closed under the partial operation taking inverse ($q \longrightarrow q^{-1}$) will be called the **rational closure** of the set A in A and will be denoted by $Div_Q A$ or $DivA$.

If M, M_1, M_2, ..., M_n are subsets of the ring Q then we define:

$$M_1 + M_2 + \cdots + M_n := \{\sum_{i=1}^{n} \pm m_i |\ m_i \in M_i\};$$

$$M_1 M_2 \ldots M_n := \{m_1 m_2 \ldots m_n |\ m_i \in M_i, i = 1, 2, \ldots, n\};$$

$$M^{-1} = \{m^{-1} |\ m \in M \cap U(Q)\}.$$

Therefore the rational closure $DivA$ is the smallest subset K of the ring Q which satisfies the following properties: a) $D \supseteq A$ and $1 \in D$, b) $D + D \subseteq D$, c) $DD \subseteq D$, d) $D^{-1} \subseteq D$.

Let Λ be an ordinal and let $(\mathbb{N}(\Lambda), +, 0)$ be the free commutative monoid with the set $\{\alpha |\ \alpha$ is an ordinal and $0 < \alpha \leq \Lambda\}$ as a basis and the ordinal 0 as the neutral element. Each element $\theta \in \mathbb{N}(\Lambda)$ can be written uniquely as the sum $\theta = \alpha_1 + \alpha_2 + \cdots + \alpha_m$, where $\Lambda \geq \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m > 0$. Let $\tau = \beta_1 + \beta_2 + \cdots + \beta_n$, $\Lambda \geq \beta_1 \geq \beta_2 \geq \cdots \beta_n > 0$ be another element from $\mathbb{N}(\Lambda)$. We shall write $\theta < \tau$, or $\tau > \theta$, iff there exist a natural number i such that

$$\alpha_1 = \beta_1, \cdots, \alpha_i = \beta_i, \quad \alpha_{i+1} < \beta_{i+1}. \tag{IV.5}$$

Here, it is supposed that $\alpha_j = 0$ for $J > m$ and $\beta_j = 0$ for $j > n$. In particular, the inequality $\beta > \alpha_n + \cdots + \alpha_m$ for an ordinal β means that $\beta > \alpha_i$ for all i. The relation $\theta \leq \tau$, as usual, means $\theta < \tau$ or $\theta = \tau$.

Theorem IV.4.1 $(\mathbb{N}(\Lambda), +, 0, \leq)$ *is a well-ordered monoid.* ∎

IV.5 The complexity

Let A be a subset of a ring Q and D be the rational closure of A in the ring Q. We shall now define subsets D_α of the ring D for any ordinal α by transfinite induction. The base of the induction construction is the definition of the following sets:

$$D_0 := \{0\}, \quad D_1 := \{0\} \cup \{\pm 1\} \cup A \cup (-A). \tag{IV.6}$$

Suppose that β is an ordinal and all sets D_α for $\alpha < \beta$ have been defined. If β is a limit ordinal then we define

$$D_\beta := \bigcup_{\alpha<\beta} D_\alpha. \tag{IV.7}$$

If $\beta = \gamma + 1$ is a non–limit ordinal then the three cases will be considered.

Case 1. D_γ is not a subgroup of $(D, +)$.

Then a smallest element $\tau_1 + \tau_2 + \cdots + \tau_n \in \mathbb{N}(\gamma)$ exists such that $D_{\tau_1} + D_{\tau_2} + \cdots + D_{\tau_n} \not\subseteq D_\gamma$ and we define

$$D_\beta := D_\gamma \cup (D_{\tau_1} + D_{\tau_2} + \cdots + D_{\tau_n}). \tag{IV.8}$$

Case 2. D_γ is a subgroup of $(D, +)$ but it is not a subring of D.

Then a smallest $\tau_1 + \tau_2 + \cdots + \tau_n \in \mathbb{N}(\gamma)$ exists such that $D_{\tau_1} D_{\tau_2} \cdots D_{\tau_n} \not\subseteq D_\gamma$ and we define

$$D_\beta := D_\gamma \cup \Big(\bigcup_{\sigma \in \pi_n} D_{\tau_{\sigma(1)}} D_{\tau_{\sigma(2)}} \cdots D_{\tau_{\sigma(n)}} \Big), \tag{IV.9}$$

where π_n denotes the group of all permutations of the symbols $1, 2, \ldots, n$.

Case 3. D_γ is a subring of the ring D but $D_\gamma^{-1} \not\subseteq D_\gamma$.

Then there exists a smallest ordinal τ, $\tau \leq \gamma$ for which $D_\gamma^{-1} \not\subseteq D_\gamma$ and we define

$$D_\beta := D_\gamma \cup D_\tau^{-1}. \tag{IV.10}$$

There will be an ordinal Λ such that D_Λ is a subring in D and $D_\Lambda^{-1} \subseteq D_\Lambda$. Then, $D_\Lambda = D$ by the definition of rational closure and we completed the construction of the set $\{D_\alpha\}$ where α runs through all the ordinals. Thus we obtain the strictly increasing sequence

$$D_0 \subset D_1 \subset D_2 \subset \ldots \subset D_\Lambda = D.$$

The **complexity**, noted $cp(d)$, of a given element $d \in D$ is the smallest ordinal number α such that $d \in D_\alpha$. If $d' \in D$ is another element and $cp(d') < cp(d)$ then we shall write $d \lhd d'$ or $d' \rhd d$ and say that d is **simpler** than d'. If d and d' have the same complexity, we shall write $d \sim d'$.

IV.6 Fully rational endomorphisms of the module of formal series and conformed decompositions

Let K be a skew field, let $M_h = hK$ be a 1–dimensional vector space for any $h \in \Gamma$ and let A be a group of monomial, σ–linear, monotone automorphisms of the module of formal series L. Let $Q = End(L_K)$ and assume $-1_L \in A$. Let D be the rational closure of A in the ring Q; an element of D will be called a **rational endomorphism**. An element $d \in D$ will be called a **fully rational**

endomorphism if for every $h \in \Gamma$ and every $e \in suppd[h]$ there exists a rational endomorphism b which is simpler than d and $b[h] = d[h]_{<e}$. If ε is an element of $\overline{\Gamma}$ (cf. section IV.2), then we denote with $\mathbf{A}_\varepsilon$ the subgroup of A consisting of all elements a in A with $V_a(\varepsilon) = \varepsilon$ and let $\mathbf{D}_\varepsilon := Div_Q A_\varepsilon$. An endomorphism $d \in D$ will be called **right ε–homogeneous** if $d \in gD_\varepsilon$ for some $g \in A$ and it will be called **left ε–homogeneous** if $d \in D_\varepsilon a$ for some $a \in A$. For any endomorphism $d \in D$ an equality $d = g(u+v)$ where $g \in A$, $u \in D_\varepsilon$ and $v \in D$ will be called a **right decomposition** of the endomorphism d at the point ε if $u \lhd d$ provided $v \neq 0$ and $V_v(\varepsilon) > \varepsilon$; similarly, an equality $d = (u+v)g$ where $g \in A$, $u \in D_\varepsilon$ and $v \in D$ will be called a **left decomposition** of the endomorphism d at the point ε if $u \lhd d$ provided $v \neq 0$ and $V_v(\varepsilon) > \varepsilon$. Let $d = g_1(u_1 + v_1)$ be a right decomposition at the point $\varepsilon \in \overline{\Gamma}$ and $d = (u_2 + v_2)g_2$ be a left decomposition at the point $\eta \in \overline{\Gamma}$. We shall say that these decompositions are **conformed** if the equality

$$P_\eta g_1 P_\varepsilon = P_\eta g_2 P_\varepsilon \tag{IV.11}$$

holds (for the notation P_η cf. page 152).

IV.7 Dubrovin's embedding

Let G be a group with **generalized cone** P, i.e. $P \subseteq G$ and

i) $PP \subseteq P$,

ii) $P \cap P^{-1} = \mathcal{U} :=$ subgroup of units of P,

iii) $P \cup P^{-1} = G$.

Let F be a skew field, assume that the group ring $F\mathcal{U}$ has a field of fractions K. Let Γ be a set of representatives of left cosets $g\mathcal{U}$ of $\mathcal{U}$ in G. Order Γ by $g_1 \leq g_2$ iff $g_1^{-1} g_2 \in P$. Consider the FG–K–module of formal power series with well ordered support $K\{\Gamma\} := \{\alpha = \sum_{h \in \Gamma} h k_h,\ k_h \in K,\ supp\ \alpha\ well\ ordered\}$. Then,

we have $FG \subseteq Q := End_K K\{\Gamma\}$. Let $D := rat_Q(FG)$ of FG in Q, i.e. D is the smallest subring of Q that contains FG with $u \in D,\ u^{-1} \in Q \longrightarrow u^{-1} \in D$. A subset $I \neq \emptyset$ of P is a **right ideal** of P iff $IP \subseteq I$. Denote by $\mathcal{O}_e(I)$ the **left order** of I, i.e. $\mathcal{O}_e(I) := \{g \in G |\ gI \subseteq I\}$. Denote by $\mathcal{UO}_e(I)$ the group of units of $\mathcal{O}_e(I)$. Lastly, consider the group ring $F\mathcal{UO}_e(I)$.

Theorem IV.7.1 (Dubrovin's embedding) *Let G be a group with generalized cone P, let F be a skew field, suppose that $F\mathcal{UO}_e(I)$ has a field of fractions K. Let Γ be a set of representatives of left cosets $g\mathcal{UO}_e(I)$ of $\mathcal{UO}_e(I)$ in G. Order Γ by $g_1 \leq g_2$ iff $g_1^{-1}g_2 \in P$. Consider the FG-K-module of formal power series with well ordered support*

$$K\{\Gamma\} := \left\{ \alpha = \sum_{h \in \Gamma} h k_h,\ k_h \in K,\ supp\ \alpha\ well\ ordered \right\}.$$

Let $D := rat_Q(FG)$ of FG in Q. Assume further that

1) P does not contain a minimal ideal,

2) $F\mathcal{UO}_e(I)$ is an Ore domain, for every right ideal I of P.

Then, $D = rat_Q FG$ is a skew field. ∎

IV.8 Application of Dubrovin's embedding to give a partial solution to Malcev's problem

Let $\mathbb{G}$ be the universal covering group of $SL(2, \mathbb{R})$. We shall use the notation Γ, $\mathbb{U}$ and x^t introduced in the definition of the universal covering group on page 152. Let F be any skew field. First we note[1] that the group $\mathbb{U}$ is an Ore

[1] cf. [KK74]

group because it possesses a torsion–free abelian normal subgroup

$$N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

with a torsion–free abelian factor group $\mathbb{U}/N \simeq (\mathbb{R}^{>0}, .)$; thus the group ring $F\mathbb{U}$ is an order into its classical skew field of fractions, which we shall denote by K. Now let us consider a family of one–dimensional right K–spaces $\{x^t K\}$, where x^t runs over Γ. Next we shall construct a module L of formal series by using the family $\{x^t K\}$. An arbitrary element from L looks like

$$\gamma = x^{t_1}k_1 + x^{t_2}k_2 + x^{t_3}k_3 + \cdots$$

where $t_1 < t_2 < t_3 < \ldots$ is a well–ordered transfinite sequence of real numbers and all k_i's are in K. L is a left F–space with a component–wise operation of multiplication. Moreover, L becomes a left $\mathbb{G}$–module if we set

$$g\gamma = x^{t_1'}(u_1k_1) + x^{t_2'}(u_2k_2) + x^{t_2'}(u_2k_2) + \cdots,$$

where $gx^{t_1} = x^{t_i'}u_i$, $u_i \in \mathbb{U} \subseteq K$.

Let A be the direct product of the groups $(F^*, .)$ and $\mathbb{G}$, i.e. $A := \{f.g | f \in F^*, g \in \mathbb{G}\}$. We may consider A as a group of monomial, σ–linear, monotone automorphisms of L_K. Let $Q = End(L_K)$ and $\mathbb{D} = Div_Q A$.

Theorem IV.8.1 (Dubrovin's partial solution to Malcev's problem) *$\mathbb{D}$ is a $\mathbb{G}$–skew field, i.e. every non–zero endomorphism of $\mathbb{D}$ is a σ–linear, fully rational and monotone automorphism which possesses right and left decompositions and these decompositions are conformed.* ∎

Bibliography

[Bir37] G. Birkhoff, *Representability of lie algebras and lie groups by matrices*, Ann. of Math **38** (1937), 526–532.

[Bir48] G. Birkhoff, *Lattice theory*, rev. ed., vol. 25, Amer. Math. Soc. Colloquium Publications, New York, 1948.

[Bok69] L. A. Bokut, *On malcev's problem*, Sibirsk. Mat. Zh **10** (1969), 965–1005.

[Bou74] N. Bourbaki, *Topologie général*, Hermann, Paris, 1974.

[Bou75] N. Bourbaki, *Groupes et algèbres de lie*, Hermann, Paris, 1975.

[Bow67] A.J. Bowtell, *On a question of malcev*, J. Algebra **9** (1967), 126–139.

[Coh61] P. M. Cohn, *On the embedding of rings in skew fields*, Proc. London Math. Soc. **11** (1961), 511–530.

[Coh63] P. M. Cohn, *Rings with a weak algorithm*, Trans. Amer. Math. Soc. **109** (1963), 332–356.

[Coh65] P. M. Cohn, *Universal algebra*, Harper and Row, New York, London, 1965.

[Coh66] P. M. Cohn, *Some remarks on the invariant basis number*, Topology **75** (1966), 215–228.

[Coh67] P. M. Cohn, *Free ideal rings*, J. Algebra **1** (1967), 410.

[Coh71a] P. M. Cohn, *The embedding of firs in skew fields*, Proc. London Math. Soc. **23** (1971), 193–213.

[Coh71b] P. M. Cohn, *Rings of fractions*, Amer. Math. Monthly **78** (1971), 596–615.

[Coh72a] P. M. Cohn, *Rings of fractions*, University of Alberta Lectures notes in Mathematics, Department of Mathematics, The University of Alberta, Edmonton, Alberta, Canada, 1972.

[Coh72b] P. M. Cohn, *Skew fields of fractions, and the prime spectrum of a general ring*, Lectures notes in mathematics, vol. 246, Springer-Verlag, Berlin, New York, 1972.

[Coh85] P. M. Cohn, *Free ring rings and their relations*, second ed., Academic Press, Inc, London, Orlando, San Diego, New York, Toronto, Montreal, Sydney, Tokyo, 1985.

[Dau70] J. Dauns, *Embeddings in division rings*, Trans. Amer. Math. Soc. **150** (1970), 287–299.

[Dic68] R. M. Dicker, *A set of independent axioms for a field and a condition for a group to be the multiplicative group of a field*, Proc. London Math. Soc. **18** (1968), 114–124.

[Dub94] N. I. Dubrovin, *The rational closure of group rings of left-ordered groups*, vol. 254, Gerhard Mercator, Universität Duisburg, Gesamthochschule, 1994.

[ES52] S. Eilenberg and N. Steenrod, *Foundations of algebraic topology*, Princeton University Press, Princeton, New Jersey, 1952.

[Fis71] J. L. Fisher, *Embedding free algebras in skew fields*, Proc. Amer. Math. Soc., vol. 42, 1971, pp. 33–35.

[FS76] D. R. Farkas and R. L. Snider, *k_0 and noetherian group rings*, J. Algebra **42** (1976), 192–198.

[Fuc63] L. Fuchs, *Partially ordered algebraic systems*, Pergamon Press, Oxford, London, New York, Paris, 1963.

[Ger79] V. N. Gerasimov, *Inverting homomorphisms of rings*, Algebra i Logika **18** (1979), 648–663.

[Ger82] V. N. Gerasimov, *Localizations in associative rings*, Sibirsk. Mat. Zh. **23** (1982), 36–54.

[Hah07] H. Hahn, *über die nichtarchimedischen Grössensysteme*, Sitzungsberichte der K. Akademie der Wissenschaften (Vienna), vol. 116, 1907, pp. 601–655.

[HB82] B. Huppert and N. Blackburn, *Finite groups II*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[Hig52] G. Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc., 3, vol. 2, 1952, pp. 326–336.

[Hig74] P. J. Higgins, *An introduction to topological groups*, London Mathematical Society Lecture Note Series, vol. 15, Cambridge University Press, Cambridge, England, 1974.

[Hil30] D. Hilbert, *Grundlagen der geometrie*, Teubner, Leipzig and Berlin, 1930.

[HS73] H. Herrlich and G. E. Strecker, *Category theory*, Allyn and Bacon, Boston, 1973.

[Hun89] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, Berlin, 1989.

[Hus66] T. Husain, *Introduction to topological groups*, W. B. Saunders Company, Philadelphia, London, 1966.

[Jac62] N. Jacobson, *Lie algebras*, Dover publications, New York, 1962.

[Jac89] N. Jacobson, *Basic algebra*, second ed., vol. I & II, W. H. Freeman and company, New York, 1989.

[KK74] A. I. Kokorin and V. M. Kopytov, *Fully ordered groups*, John Wiley & Sons, New York, Toronto, 1974.

[Kle67] A. A. Klein, *Rings nonembeddable in fields with multiplicative semigroups embeddable in groups*, J. Algebra **9** (1967), 100–125.

[Lam91] T. Y. Lam, *A first course in noncommutative rings*, Springer–Verlag, New York, Berlin, Heidelberg, London, Paris, 1991.

[Lan93] S. Lang, *Algebra*, third ed., Addison Wesley, Reading, Massachusetts, Menlo Park, California, New York, 1993.

[Lev42] F. W. Levi, *Ordered groups*, Proceedings of the Indian Academy of Sciences, vol. 16, 1942, pp. 256–263.

[Lic94] A. I. Lichtman, *Valuation methods in division rings*. To appear in J. of Algebra, 1994.

[LL77] J. Lewin and T. Lewin, *An embedding of the group algebra of a torsion free one relator group in a field*, J. Algebra **43** (1977), 202–212.

[Mal37] A. I. Malcev, *On the immersion of an algebraic ring into a field*, Math. Ann. **113** (1937), 686–691.

[Mal48] A. I. Malcev, *The embedding of group algebras into division algebras*, Doklady Nauk USSR **60** (1948), 1499–1501.

[Mal78] P. Malcolmson, *A prime matrix ideal yields a skew field*, J. London Math Soc. **18** (1978), 221–233.

[Mal80] P. Malcolmson, *Determining homomorphisms into a skew field*, J. Algebra **64** (1980), 399–413.

[Mal82] P. Malcolmson, *Construction of universal matrix localizations*, Lectures notes in mathematics, vol. 951, Springer-Verlag, Berlin, New York, 1982.

[Mal84] P. Malcolmson, *Matrix localizations of firs*, Tans. Amer. Math. Soc. **282** (1984), 503–518, 519–527.

[MKS76] W. Magnus, W. Karras, and D. Solitar, *Combinatorial group theory*, Dover, New York, 1976.

[ML71] S. Mac Lane, *Categories for the working mathematician*, Springer-Verlag, New York, Heidelberg, Berlin, 1971.

[Mou37] R. Moufang, *Einige untersuchungen über geordnete Schiefkörper*, Journal für Mathematik **176** (1937), 203–223.

[MR87] J. C. McConnell and J. C Robson, *Noncommutative noetherian rings*, John Wiley & Sons, Chichester, New York, Brisbane, Toronto, Singapore, 1987.

[Neu49a] B. H. Neumann, *On ordered division rings*, Trans. Amer. Math. Soc **66** (1949), 202–252.

[Neu49b] B. H. Neumann, *On ordered groups*, Amer. J. Math **71** (1949), 1–18.

[Ore31] O. Ore, *Linear equations in non-commutative fields*, Ann. Math **32** (1931), 463–477.

[Rab37] D. G. Rabinow, *Independent set of postulates for abelian groups and fields in terms of the inverse operations*, Amer. J. Math. **59** (1937), 211–224.

[Sch50] O. F. G. Schilling, *The theory of valuations*, Amer. Math. Soc., Providence, R. I., 1950.

[Sch85] A. H. Schofield, *Representations of rings over skew fields*, London Mathematical Society Lecture Note Series, vol. 92, Cambridge University Press, Cambridge, London, New York, New Rochelle, Melbourne, Sydney, 1985.

[Str75] B. Strenstrom, *Rings of quotients*, Springer-Verlag, Berlin, 1975.

[Tam53] D. Tamari, *On the embedding of Birkhoff-Witt rings in quotients fields*, Proc. Amer. Math. Soc. **4** (1953), 197–202.

[War89] S. Warner, *Topological fields*, Mathematics Studies, vol. 157, North Holland, Amsterdam, New York, Oxford, Tokyo, 1989.

[Wit37] E. Witt, *Treue darstellung liescher ringe*, J. reine angew. Math. **177** (1937), 152–60.

[ZS60] O. Zariski and P. Samuel, *Commutative algebra*, vol. 2, D. Van Nostrand Company, Princeton, New Jersey; Toronto, London, 1960.

Name Index

Birkhoff, G., 52, 107
Blackburn, N., 63
Bokut, L. A., 91
Bourbaki, N., 78, 84, 105
Bowtell, A. J., 91

Cohn, P. M., 1, 50, 51, 86, 91, 108, 113, 118, 144, 146–148, 150

Dauns, J., 86
Dicker, R. M., 86
Dubrovin, N. I., 149

Eilenberg, S., 88

Farkas, D. R., 65
Fisher, J. L., 2
Fuchs, L., 52

Gerasimov, V. N., 112, 120

Hahn, H., 50
Herrlich, H., 88, 113
Higgins, P. J., 78
Higman, G., 50
Hilbert, D., 50
Hungerford, T. W., 21, 75, 117, 119, 131
Huppert, B., 63
Husain, T., 78

Jacobson, N., 105, 106

Karrass, W., 63
Klein, A. A., 91
Kokorin, A. I., 159
Kopytov, V. M., 159

Lam, T. Y., 41–43
Levi, F. W., 52
Lewin, J., 65
Lewin, T., 65
Lichtman, A. I., 52

Mac Lane, S., 88, 113
Magnus, W., 63
Malcev, A. I., 50, 91
Malcolmson, P., 112
McConnell, J. C., 43
Moufang, R., 50, 73, 74

Neumann, B. H., 50, 52

Ore, O., 1, 20

Rabinow, D. G., 86
Robson, J. C., 43

Samuel, P., 91, 102
Schilling, O. F. G., 91
Schofield, A. H., 113
Snider, R. L., 65
Solitar, D., 63
Steenrod, N., 88
Strecker, G. E., 88, 113
Strenstrom, B., 21

Tamari, D., 51

Warner, S., 78
Witt, E., 107

Zariski, O., 91, 102

Index

$(\Gamma, \leq)$, 151
A, 151
A_ϵ, 152
P_ϵ, 152
R–subring
    local, 114
$U(P)$, 152
V, 151
$\overline{\Gamma}$, 151
$\preceq$, 154
2–cocycle, 106

adic topology, 45
archimedean class, 69
associated graded ring, 102

beginning, 154
Birkhoff–Witt algebras, 105
BW–algebra, 105

cancellation by T, 6
cancellation monoid, 6
cancellative subset, 5
canonical homomorphism, 113
category
    of R–fields and specializations, 115
    of epic R–fields and specializations, 117
    of R–rings, 113
Cauchy filter, 84
Cauchy filter base, 84
centralizer, 29
chain, 53
classical quotient ring, 28
coherence conditions, 88
complete, 84
completely prime ideal, 118
complex–skew polynomial ring, 41
complexity, 157
component, 154
cone, *see* positive cone
conformed decomposition, 158
congruence relation, 87
convergence of a filter, 84
converges, 154
Cramer's rule for non–commutative rings, 126

crossed product, 44
cutting, 154

DCC, 65
Dedekind closure, 151
Dedekind cut, 151
degree, 32
degree function, 32
denominator, 25, 126
denominator set, 2
derivation, 39
determinantal sum, 134
diagonal sum, 134
differential polynomial rings, 31
dual assertion, 52
dual order–isomorphism, 53
dual partially ordered set, 52

$\mathcal{E}_R$, 117
epic R–field, 114
epic ring homomorphism, 114
ε–beginning, 154
ε–cutting, 154
equivalence of local homomorphism between epic R–fields, 115
eventually constant, 65
extending by continuity, 85

f. o. set, 53
$\mathcal{F}_R$, 115
field of fractions, 21, 114
universal epic, 118
filter, 80
filter base, 80
filtered ring, 101
filtration, 101
finite sums, 69
formal Laurent series, 45
formal power series, 44, 68
free metabelian group, 73
Frobenius endomorphism, 43
full matrix, 135
full order, 53
fully ordered set, 53
fully rational endomorphism, 157
fundamental system of neighbourhoods, 80

G–skew field, 160
G1., 53
G2., 53
G3., 53
generalized cone, 158
generated filter, 80
GL., 54
GR., 54
group of fractions, 2
group topology, 78

h–component, 154
h–homogeneous, 153

Hilbert's twist, 33
homeomorphism, 79
homogeneous beginning, 153
homogeneous series, 153
homogeneous space, 79
homomorphism
    epic ring, 114
    local, 114
    R–ring, 113
    Σ–inverting, 120
    T–inverting monoid, 2
    T-inverting ring, 19
    universal Σ–inverting, 120
homomorphism
    R–ring, 21

incomparable, 53
induced partial order, 53
infinitely larger, 69
infinitely smaller, 69
integral element, 54
integral part, 54
inverse limit, 88
inverse system, 88
isotone, 53

Jacobi–identity, 106

l. o. group, 54
least matrix ideal containing a given set $\mathcal{X}$, 138
left decomposition, 158
left ε–homogeneous, 158
left fractions, 23
left multiplication, 79
left order of an ideal, 159
left ordered group, 54
left Ore domain, 28
left Ore set for a ring, 24
left skew polynomial ring, 35
left translation, 79
length, 76
Lie algebra, 106
linear order, 53
linearly ordered set, 53
local homomorphism, 114
local ring, 115
localization
    for commutative monoids, 6
    of R at the set T, 20
localization at the set of invertible matrices, 122
localization at the set of singular matrices, 122
loset, 53

matrix ideal, 136
matrix ideal generated by $\mathcal{X}$, 138
matrix pre–ideal, 135
matrix pre–ideal generated by $\mathcal{X}$, 138
module of formal series, 153

monoid of fractions, 2
monomial, 155
monotone, 155
multiplicative, 123

negative, 54
neighbourhood, 80
non–full matrix, 135
normal subsemigroup, 55
numerator, 25, 126

o. group, 53
order, 44
order extension, 53
order preserving, 53
order–homomorphism, 53
order–isomorphic, 53
order–isomorphism, 53
ordered group, 53
Ore domain, 28

p. o. set, 52
P1., 52
P2., 52
P3., 52
P4., 53
partial order, 52
partially ordered set, 52
PC1., 54
PC2., 54
PC3., 54
Poincare–Birkhoff–Witt theorem, 107
polycyclic group, 65
positive, 54
positive cone, 54
preorder, 53
prime matrix ideal, 141
product of matrix ideals, 140
projection, 153
projective limit, 88
projective system, 88
proper ε–beginning, 154
proper matrix pre–ideal, 136
pseudo–valuation, 102

quasiorder, 53
quaternion algebra, 42
quotient semigroup, 88

R–field, 113
  epic, 114
    universal, 117
R–ring, 20, 113
  homomorphism, 113
  homomorphisms, 21
R–subring, 114
r. o. group, 54
radical of a matrix ideal, 142
rational closure, 123, 155
rational endomorphism, 157
regular element, 28

regular set, 28
regular topological space, 84
regular topology, 84
relatively archimedean, 69
residue–class field, 115
reverse order, 53
right decomposition, 158
right denominator set for a ring, 23
right ϵ–homogeneous, 158
right fractions, 23
right ideal of a positive cone, 159
right ordered group, 54
right Ore condition for rings, 23
right Ore domain, 28
right Ore set, 8
right Ore set of a ring, 23
right reversible, 23
ring of constants, 39
ring of fractions, 19
RPC1., 56
RPC2., 56
RPC3., 56

$S(x_1, x_2, \ldots, x_n)$, 60
$S^G(x_1, x_2, \ldots, x_n)$, 60
semifirs, 147
semiprime matrix ideal, 141
shift automorphism, 43
Σ–inverting homomorphism, 120
σ–linear, 154
Σ–rational closure, 123
simpler, 157
singular kernel, 121
singular matrix over a skew field, 119
skew Laurent polynomial, 44
skew Laurent series, 45
skew polynomial ring, 33
small, *see* V–small
smallest element, 53
specialization, 115
strongly prime ideal, 118
sum, 154
summable, 154
support, 68
symmetric, 83

tensor ring, 32
TG 1, 78
TG 2, 78
TG 3, 79
TGB 1, 82
TGB 2, 82
TGB 3, 82
TGN 1, 80
TGN 2, 80
TGN 3, 80
topological group, 78
topological group morphism, 78
total order, 53

total quotient ring, 28
totally ordered set, 53
translation ring, 43
trivial order, 53
twisted group ring, 69
twisted Laurent series, 45
twisted polynomial rings, 31

universal covering group, 153
universal epic field of fractions, 118
universal epic R–field, 117
universal group, 2
universal localizations, 120
universal Σ–inverting homomorphism, 120
universal Σ–inverting ring, 120
universal T–inverting monoid, 2
universal T–inverting ring, 20
untwisted ring of formal power series, 69

V–small, 84
V.1, 91
V.2, 91
V.3, 91
valuated ring, 91
valuation, 44, 91

well–ordered, 53
Weyl algebra, 42

x–adic topology, 45